Department of Electrical Engineering and Automation

# Wireless 5G for Medium-Voltage Grid IEC 61850 based Protection Communication

Petra Raussi Chauhan

Aalto University

DOCTORAL THESES

Aalto University publication series
**DOCTORAL THESES** 152/2023

# Wireless 5G for Medium-Voltage Grid IEC 61850 based Protection Communication

**Petra Raussi Chauhan**

A doctoral thesis completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Electrical Engineering, at a public examination held at the lecture hall AS1 of the school on 13 October 2023 at 12.

**Aalto University**
**School of Electrical Engineering**
**Department of Electrical Engineering and Automation**
**Power systems and High Voltage Engineering**

**Supervising professor**
Prof. Matti Lehtonen, Aalto University, Finland

**Thesis advisor**
Research Prof. D.Sc. Kari Mäki, VTT Technical Research Centre of Finland, Finland

**Preliminary examiners**
Dr. Haiyu Li, University of Manchester, UK
Prof. Mohammed Elmusrati, University of Vaasa, Finland

**Opponent**
Assoc. Prof. Mohamed F. M. Abdel-Fattah, Reykjavik University, Iceland

Aalto University publication series
**DOCTORAL THESES** 152/2023

ISBN 978-952-64-1441-6 (printed)
ISBN 978-952-64-1442-3 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-64-1442-3

Images: Cover photo by VTT Technical Research Centre of Finland

Unigrafia Oy
Helsinki 2023

Finland

NORDIC SWAN ECOLABEL
Printed matter
4041-0619

A! Aalto University

**Abstract**

**Aalto University, P.O. Box 11000, FI-00076 Aalto** www.aalto.fi

**Author**
Petra Raussi Chauhan

**Name of the doctoral thesis**
Wireless 5G for Medium-Voltage Grid IEC 61850 based Protection Communication

**Publisher** School of Electrical Engineering

**Unit** Department of Electrical Engineering and Automation

**Series** Aalto University publication series DOCTORAL THESES 152/2023

**Field of research** Power Systems and High Voltage Engineering

**Manuscript submitted** 18 June 2023 **Date of the defence** 13 October 2023

**Permission for public defence granted (date)** 25 August 2023 **Language** English

□ **Monograph** ☒ **Article thesis** □ **Essay thesis**

**Abstract**

To combat climate change, a large amount of carbon-neutral renewable energy production must be integrated into the power system. The most techno-economically affordable solution to accomplish renewable integration is to increase system intelligence by interfacing communication networks with power systems to form a smart grid. Historically grid automation has been hardwired as earlier wireless technologies lacked the reliability required by protection applications. Fifth generation cellular network (5G) promises to reach low latency and high reliability, suitable for protection communication but needs validation whether promised targets are met in practice. Typically, studies on wireless technologies for smart grid applications are simulations, lacking the accuracy of commercially available wireless networks. Thus, protection communication via 5G is the main focus of this thesis.

The aim of this thesis is to investigate whether commercially available 5G is applicable for protection communication. This topic is divided into three sub-research questions discussed in this thesis and the publications. Firstly, prior bottlenecks of wireless technologies for protection communication 5G removes are identified. These include a lack of reliability and low latency, which could be resolved by 5G use cases with associated service portfolios, network slicing, and edge computing. The controller-hardware-in-the-loop (CHIL) results show significant improvement in successfully protected faults with 5G standalone (SA); also, fault clearance times are not as widely spread and slanted towards the lower times.

Secondly, the thesis identifies limitations hindering 5G's use in protection communication. These include a small packet size of IEC 61850-based messages compared to the optimal size for 5G and a lack of granularity in the network slicing implementations. Substation communication consists of traffic types with diverse requirements, and adding all the traffic into one slice can increase delays and packet loss in protection communication. Furthermore, edge computing will increase the complexity of protection and collaboration with telecommunication providers requiring applicability to be assessed carefully.

Thirdly, the thesis proposes approaches to mitigate the identified limitations. IEC 61850-based packet sizes could be optimised by aggregating packets under the same Ethernet header for wireless transmission. If slicing lacks granularity, protection communication could be prioritised by overall prioritisation of all traffic and adjustment of individual traffic sources. The CHIL results show that prioritisation improves the reliability of protection communication without impacting latency. Additionally, the suitability of edge computing is assessed by a computational study highlighting the bottleneck of total uplink traffic in the urban scenario and the lack of density of devices in the rural scenario.

**Keywords** 5G, Cellular Networks, Fault Indication, Grid Automation, IEC 61850, Protection, Reliability, Wireless Technology

**ISBN (printed)** 978-952-64-1441-6 **ISBN (pdf)** 978-952-64-1442-3

**ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

**Location of publisher** Helsinki **Location of printing** Helsinki **Year** 2023

**Pages** 133 **urn** http://urn.fi/URN:ISBN:978-952-64-1442-3

Aalto-yliopisto

**Tiivistelmä**

**Aalto-yliopisto, PL 11000, 00076 Aalto** www.aalto.fi

**Tekijä**
Petra Raussi Chauhan

**Väitöskirjan nimi**
Langaton 5G keskijänniteverkon IEC 61850 pohjaisessa suojauskommunikaatiossa

**Julkaisija** Sähkötekniikan korkeakoulu

**Yksikkö** Sähkötekniikan ja automaation laitos

**Sarja** Aalto University publication series DOCTORAL THESES 152/2023

**Tutkimusala** Sähköverkot ja suurjännitetekniikka

**Käsikirjoituksen pvm** 18.06.2023 **Väitöspäivä** 13.10.2023

**Väittelyluvan myöntämispäivä** 25.08.2023 **Kieli** Englanti

□ **Monografia** ☒ **Artikkeliväitöskirja** □ **Esseeväitöskirja**

**Tiivistelmä**

Ilmastonmuutoksen hillitsemiseksi suuri määrä hiilineutraalia uusiutuvaa energian tuotantoa on liitettävä sähköverkkoon. Teknistaloudellisesti halvin ratkaisu uusiutuvan liittämiseksi on järjestelmän älykkyyden lisääminen yhdistämällä tietoliikenne- ja sähköverkot muodostamaan älykäs sähköverkko. Historiallisesti verkkoautomaatio on ollut johdotettua koska aiemmista langattomista teknologioista on puuttunut suojaussovellusten tarvitsema luotettavuus.

5G-teknologia lupaa saavuttaa matalan viiveen ja korkean luotettavuuden, jolloin se olisi sopiva suojauskommunikaatioon, mutta luvattujen tavoitteiden täyttyminen täytyy varmistaa käytännössä. Yleensä langatonta teknologiaa älykkään sähköverkon sovelluksille tutkitaan simuloimalla, jossa ei voida huomioida kaupallisten langattomien verkkojen oikeellisuutta. Siksi suojauskommunikaatio 5G:llä on tämän työn aiheena.

Väitöskirjan tavoitteena on selvittää, soveltuuko kaupallinen 5G suojauskommunikaatioon. Aihe on jaettu kolmeen alakysymykseen, joista ensimmäinen on suojauskommunikaatiolle aiempien langattomien teknologioiden haasteiden, jotka 5G ratkaisee, tunnistaminen. Näitä haasteita ovat luotettavuuden ja matalan viiveen puute, mitkä voidaan ratkaista 5G käyttötapauksilla ja näiden palveluvalikoimilla, verkon viipaloinnilla ja reunalaskennalla. Tulokset simuloinnista, jossa laitteisto on osa silmukkaa (hardware-in-the-loop), osoittavat huomattavan parannuksen suojatuissa vioissa itsenäisessä 5G Standalone -verkossa sekä vian erotusaikojen hajonnassa ja kallistumisessa kohti matalampia aikoja.

Toiseksi väitöskirja tunnistaa rajoitteita 5G:n käytössä suojauskommunikaatiossa, kuten IEC 61850-pohjaisten viestien pienen pakettikoon verrattuna 5G:n ihanteelliseen pakettikokoon sekä hienojakeisuuden puutteeseen verkon viipalointitoteutuksissa. Sähköasemakommunikaatio koostuu tietoliikennelajeista, joilla on monipuoliset vaatimukset, ja liittämällä kaiken liikenteen yhdelle viipaleelle viiveet ja pakettihäviö suojauskommunikaatiossa voivat kasvaa. Lisäksi reunalaskenta lisää suojauksen monimutkaisuutta ja vaadittavaa yhteistyötä teleoperaattorien kanssa, joten reunalaskennan soveltuvuutta täytyy arvioida huolellisesti.

Kolmanneksi väitöskirja esittää ratkaisuja tunnistettujen rajoitteiden lieventämiseksi. IEC 61850-pohjaisia pakettikokoja voitaisiin tehostaa kokoamalla paketteja saman Ethernet-otsakkeen alle langattoman tiedonsiirron ajaksi. Jos viipaloinnin hienojakeisuus on puutteellista, suojauskommunikaatio voitaisiin asettaa etusijalle sekä koko liikenteen asettelussa tärkeysjärjestykseen että yksittäisten liikennelähteiden mukauttamisella. Tulokset osoittavat, että suojauksen etusijalle asettelu kasvattaa suojauskommunikaation luotettavuutta ilman vaikutuksia viiveisiin. Lisäksi reunalaskennan soveltuvuutta arvioitiin laskennallisilla tutkimuksilla, joiden tulokset korostavat kokonaissiirtoyhteyden ylöspäin olevan haaste kaupunkitapauksessa ja

**Avainsanat** 5G, IEC 61850, langaton teknologia, luotettavuus, soluverkko, suojaus, verkkoautomaatio, vian ilmaisu

**ISBN (painettu)** 978-952-64-1441-6 **ISBN (pdf)** 978-952-64-1442-3

**ISSN (painettu)** 1799-4934 **ISSN (pdf)** 1799-4942

**Julkaisupaikka** Helsinki **Painopaikka** Helsinki **Vuosi** 2023

**Sivumäärä** 133 **urn** http://urn.fi/URN:ISBN:978-952-64-1442-3

# Acknowledgements

The research work presented in this doctoral thesis was conducted at the IntelligentEnergy testbed of Smart Grids team at VTT Technical Research Centre of Finland. This work was financed by European Commission in H2020 ERIGrid (No. 654113) project, Business Finland in 5GVIIMA (6392/31/2018) and IFORGE (7263/31/2021) projects, Ministry of Economic Affairs and Employment of Finland in Smart Energy Spearhead project, and VTT Technical Research Centre of Finland in finalizing this doctoral thesis.

First, I would like to thank my supervisor Prof. Matti Lehtonen for giving me the freedom to explore an interesting research topic and providing prompt responses when I needed support and guidance. I would also like to thank my thesis advisor D.Sc. Kari Mäki for providing a continuous stream of funding to enable this research work.

I am very thankful for the pre-examiners, Dr. Haiyu Li, University of Manchester, and Prof. Mohammed Elmusrati, University of Vaasa, for providing constructive feedback that improved the quality of this thesis. I would also like to thank Assoc. Prof. Mohamed F.M. Abdel-Fattah, Reykjavik University, for acting as the opponent in the public examination of this thesis.

"If I have seen further it is by standing on the shoulders of giants."
- Isaac Newton, 1675

As I. Newton has previously remarked, I want to express my gratitude to the connectivity researchers I have had the honor to work with: Heli Kokkoniemi-Tarkkanen, Kimmo Ahola, Dr. Jorma Kilpi, Sami Ruponen, Seppo Horsmanheimo, Lotta Tuomimäki, Antti Heikkinen, and Mikko Uitto. Many thanks for allowing me to stand on your shoulders to reach novelty. Especially Heli for being my partner in the lab; words cannot describe my appreciation for all our thought-provoking late-evening discussions while the measurements were running. Similarly, I would like to thank the cyber security researchers: L.Sc. Juha Pärssinen, Sami Noponen, Pia Raitio, and Jarno Salonen. It was always a pleasure to have you hack into the system and study the environment from a totally different perspective. I would also like to thank Mikael Opas for being my left hand in the lab and for all the configurations, installations, and support with the measurements. Without you, I would not have accomplished half of what we have. Many thanks to Jarmo Kuusisto for all the installation work, electrical and otherwise. I want to express my gratitude to Dr. Kalle Rauma for kindly giving

me his superior tips on journal paper writing when I thought I had reached my limit in scientific writing. I would also like to thank Jonna Tammikivi for bringing her energy of joy, laughter, and sunshine to the lab, figuratively and literally, and for her tips on AI tools. Many thanks also to Ville Ollikainen and D.Sc. Katja Sirviö for peer support and clarifying discussions during the writing process of this thesis.

I am grateful for the co-authors from outside of VTT: Seppo Borenius of Aalto University, Petri Hovila of ABB, D.Sc. Anna Kulmala of ABB, Saifullah Shafiq of University of Queensland, Bilal Khan of Concordia University, and Dr. Ali Taleb Al-Awami of K.A. CARE Energy Research & Innovation Center. Especially Petri for his continued championing of this research topic and the insights into protection, and Anna for her mentoring and advice.

I would especially like to thank my family for their support through this thesis and life. My mother, Katri, for her unconditional love and support. Thanks to her patience in teaching me that I am not incapable of solving math and science problems, I am writing this doctoral thesis acknowledgement today. My father, Ari, for grounding me with our discussions on practical electrical and electrical safety challenges from the field. My brothers, Perttu and Sakari, and their spouses and child for their humor and support. I would also like to express my appreciation for my mother-in-law, Karuna, for her patience and high regard for higher education, and my brother-in-law, Pulkit, for his superior management skills, without which it would have been impossible to accomplish a whirlwind wedding and doctoral thesis within a spring. Additionally, many thanks to my pseudo family, Aruna, Vijay, Atulya, and Amulya, for welcoming me and my brothers with open arms and alleviating stress during this spring.

Last but not least, I would like to express my deepest gratitude to my husband, D.Sc. Vardaan Chauhan, for always encouraging me to reach new heights I couldn't have imagined by myself and for all the insightful discussions during these doctoral studies. For all the years sacrificed in different addresses, I highly appreciate you for remaining a constant in my life, even when this research has taken me countless times away from you. I am blessed to have you in my life and can't wait to grow our family with you and Loki.

Jyväskylä, 7 September 2023
Petra Raussi Chauhan

# Contents

# List of Abbreviations and Symbols

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| 4G | Fourth-Generation Cellular Network |
| 5G | Fifth-Generation Cellular Network |
| $B$ | bandwidth capacity |
| CHIL | Controller-Hardware-in-the-Loop |
| CIGRE | International Council on Large Electric Systems |
| $C_T$ | total unavailable bandwidth at the moment $T$ |
| DSO | Distribution System Operator |
| eMBB | enhanced Mobile Broadband |
| EV | Electric Vehicle |
| $f$ | amount of traffic per traffic type |
| GOOSE | Generic Object-Oriented Substation Event |
| GSA | Global mobile Suppliers Association |
| GSM | Global System for Mobile Communications |
| HIL | Hardware-in-the-Loop |
| HTB | Hierarchical Token Bucket |
| ICT | Information and Communication Technology |
| IEC | International Electrotechnical Commission |
| IED | Intelligent Electronic Device |
| IoT | Internet of Things |
| IP | Internet Protocol |
| KPI | Key Performance Indicator |
| LTE | Long-Term Evolution |
| MAC | Media Access Control |

| | |
|---|---|
| MMS | Manufacturing Message Specification |
| mMTC | massive Machine Type Communication |
| $n_{ED\_MIN}$ | minimum number of edge devices |
| $n_{FL}$ | number of feeder lines at a substation on average |
| $n_{MU}$ | number of merging units |
| $n_{PS}$ | number of primary substations |
| NSA | Non-Standalone |
| $n_{SS}$ | number of secondary substations |
| OSI | Open Systems Interconnection |
| OT | Operational Technology |
| QoS | Quality of Service |
| RAN | Radio Access Network |
| $r_{total\_UP}$ | total uplink traffic rate |
| $r_{UPpMU}$ | uplink traffic rate per merging unit |
| SA | Standalone |
| SCADA | Supervisory Control and Data Acquisition |
| SCL | Substation Configuration Language |
| SLA | Service Level Agreement |
| SuT | System under Test |
| SV | Sampled Value |
| TB | Technical Brochure |
| TLV | Type, Length, Value |
| URLLC | Ultra-Reliable Low-Latency Communication |
| VPN | Virtual Private Network |
| WLAN | Wireless Local Area Network |
| $x$ | priority indication as a weight |
| XML | Extensible Markup Language |

# List of Publications

This doctoral dissertation consists of a summary and of the following publications which are referred to in the text by their numerals.

**1.** Raussi, P., Kilpi, J., Kokkoniemi-Tarkkanen, H., Kulmala, A., Hovila, P. 2022. Edge Computing supported Fault Indication in Smart Grid. In *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Singapore, Singapore, pp. 278-283, October 2022. DOI: 10.1109/SmartGridComm52983.2022.9960979

**2.** Kokkoniemi-Tarkkanen, H., Raussi, P., Horsmanheimo, S., Hovila, P., Kulmala, A., Borenius, S. 2023. 5G Edge for Power System Applications. In *International Conference on Electricity Distribution (CIRED)*, Rome, Italy, June 2023. DOI: *Accepted for proceedings*.

**3.** Raussi, P., Kokkoniemi-Tarkkanen, H., Ahola, K. 2022. Methodology to Decrease Packet Loss in IEC 61850 Substation Communication over Wireless 5G Communication. *CIGRE Science and Engineering*, number 26, pp. 117-128, November 2022.

**4.** Raussi, P., Pärssinen, J., Noponen, S., Opas, M., Raitio, P., Salonen, J. 2022. Impact of Cyber-Attacks on Process Bus and Time Synchronisation Communication at Substations. In *CIGRE 2022 Kyoto Symposium*, Kyoto, Japan, pp. 1-10, April 2022.

**5.** Pärssinen, J., Raussi, P., Noponen, S., Opas, M., & Salonen, J. 2022. The Digital Forensics of Cyber-Attacks at Electrical Power Grid Substation. In *10th International Symposium on Digital Forensics and Security (ISDFS 2022),* Istanbul, Turkey, pp. 1-6, June 2022. DOI: 10.1109/ISDFS55398.2022.9800831

**6.** Shafiq, S., Khan, B., Raussi, P., Taleb Al-Awami, A. 2021. A Novel Communication-Free Charge Controller for Electric Vehicles Using Machine Learning. *IET Smart Grid*, vol. 4, number 3, pp. 334-345, March 2021. DOI: 10.1049/stg2.12032

**7.** Raussi, P., Kokkoniemi-Tarkkanen, H., Ahola, K., Heikkinen, A., Uitto, M. 2023. Prioritizing Protection Communication in a 5G Slice: Evaluating HTB Traffic Shaping and UL Bitrate Adaptation for Enhanced Reliability. *The Journal of Engineering*, volume 2023, number 9, pp. 1-18, September 2023. DOI: 10.1049/tje2.12309

# Author's Contribution

**Publication 1:** "Edge Computing Supported Fault Indication in Smart Grid"

The main idea was developed by Petra Raussi and Heli Kokkoniemi-Tarkkanen. Jorma Kilpi helped to improve the content, especially the general background on edge computing, assisted in mathematical representations and formulation of the edge scenarios, and developed the step function. Heli Kokkoniemi-Tarkkanen was responsible for the communication test setup, and she established the QoS measurement system, verified and analysed the QoS measurement findings, and visualised the QoS results. Petra Raussi was responsible for implementing the CHIL experiments, analysing the CHIL findings, and writing the paper with the support of Heli Kokkoniemi-Tarkkanen and Jorma Kilpi. Anna Kulmala and Petri Hovila provided comments on the paper.

**Publication 2:** "5G Edge for Power System Applications"

The main idea was developed by Heli Kokkoniemi-Tarkkanen and Petra Raussi. Petri Hovila, Anna Kulmala, and Seppo Borenius helped to improve the content. Seppo Borenius contributed to the section on 5G and edge computing. Seppo Horsmanheimo contributed the sections on the current deployment state of 5G SA and on SA vs. NSA, implemented the Nemo measurements, analysed the Nemo findings, and visualised the Nemo results. Heli Kokkoniemi-Tarkkanen contributed the 5G communication and edge computing considerations, was responsible for communication test setup, performed QoS measurements, verified and analysed the QoS measurement findings, visualised the QoS results, and was responsible for writing the paper. Petra Raussi was responsible for implementing the CHIL experiments, analysing the CHIL findings, and contributing literature review on prior applications of edge computing on smart grids and the suitable smart grid applications for edge computing. Anna Kulmala, Petri Hovila, and Seppo Borenius provided comments on the paper.

**Publication 3:** "Methodology to Decrease Packet Loss in IEC 61850 Substation Communication over Wireless 5G Communication"

The main idea was developed by Heli Kokkoniemi-Tarkkanen and Petra Raussi. Kimmo Ahola developed the data aggregation implementation. Heli Kokkoniemi-Tarkkanen was responsible for the communication test setup, and she performed QoS measurements, verified and analysed the QoS measurement findings, and visualised the QoS results. Petra Raussi was responsible for implementing the CHIL experiments, analysing the CHIL findings, and writing the paper with the support of Heli Kokkoniemi-Tarkkanen and Kimmo Ahola. Petra Raussi acquired funding for the project.

**Publication 4:** "Impact of Cyber Attacks on Process Bus and Time Synchronisation Communication at Substations"

The main idea was developed by Petra Raussi. Juha Pärssinen developed the attack implementations and helped to improve the content, analysed the attack findings, and visualised the attack results. Mikael Opas assisted in implementing the CHIL experiments, analysed the CHIL findings, and visualised the CHIL results. Sami Noponen helped to improve the content on mitigation actions. Petra Raussi was responsible for implementing the CHIL experiments, analysing the CHIL findings, and writing the paper. Pia Raitio and Jarno Salonen provided comments on the paper.

**Publication 5:** "The Digital Forensics of Cyber Attacks at Electrical Power Grid Substation"

Juha Pärssinen developed the main idea and the attack implementations, analysed the attack findings, visualised the attack results, and was responsible for writing the paper. Mikael Opas assisted in implementing the CHIL experiments. Sami Noponen helped to improve the content. Petra Raussi helped to improve the content for the power systems aspects and was responsible for implementing the CHIL experiments. Jarno Salonen provided comments on the paper.

**Publication 6:** "A Novel Communication-Free Charge Controller for Electric Vehicles Using Machine Learning"

The main idea was developed by Saifullah Shafiq and Bilal Khan. Saifullah Shafiq and Bilal Khan developed the controller, implemented the simulations, analysed the findings, and visualised the results. Petra Raussi assisted in implementing the simulations by developing the laboratory environment which enabled realisation of the simulations, provided suggestions to improve the idea to ensure that the simulations could be implemented in the laboratory environment, run simulations and collected corresponding result data after the research visit, and provided comments to improve the content of the paper. Saifullah Shafiq and Bilal Khan were responsible for writing the paper under the guidance of Ali Taleb Al-Awami.

**Publication 7:** "Prioritizing Protection Communication in a 5G Slice: Evaluating HTB Traffic Shaping and UL Bitrate Adaptation for Enhanced Reliability"

The main idea was developed by Petra Raussi and Heli Kokkoniemi-Tarkkanen. Kimmo Ahola developed the HTB prioritisation implementation. Antti Heikkinen and Mikko Uitto developed the live video stream adaptation system. Heli Kokkoniemi-Tarkkanen was responsible for the communication test setup, and she performed QoS measurements, verified and analysed the QoS measurement findings, and visualised the QoS results. Petra Raussi was responsible for representing the prioritisation mathematically, implementing the CHIL experiments, analysing the CHIL findings, visualising the CHIL results, and writing the paper with support from Heli Kokkoniemi-Tarkkanen, Kimmo Ahola, Antti Heikkinen, and Mikko Uitto. Heli Kokkoniemi-Tarkkanen, Kimmo Ahola, Antti Heikkinen, and Mikko Uitto provided comments on the paper.

# 1. Introduction

## 1.1 Background

Anthropogenic climate change is one of the great challenges of the current era. To combat this challenge, nations have set ambitious climate targets to mitigate and adapt to the consequences of climate change [1]. The energy sector is the largest segment of emissions [2]. To meet the ambitious targets for the energy sector, a large amount of carbon-neutral renewable energy production must be integrated into the power system. The most techno-economically affordable solution to accomplish renewable integration is to increase system intelligence by irrecoverably interfacing information and communication technology (ICT) infrastructure with power systems to form a smart grid. With increased intelligence in the grid, the efforts to maximise the capacity in grid planning can be shifted to optimisation, thus reducing the demand for new materials. Furthermore, increased intelligence can enable local energy communities and other flexibility solutions to support grid stability.

Historically, power systems communication infrastructure has consisted of hardwired copper connections. The early applications mostly consisted of dedicated connections between two devices. For instance, most protection relays were implemented to operate independently based on local grid measurements. For example, in substation automation, connectivity to current and voltage transformers and breakers was first hardwired and then implemented with wired Ethernet connections at the station and process bus, as portrayed in Figure 1. Earlier wireless technologies were not considered for power system applications due to a lack of reliability compared to wired connectivity. However, many proposals and validation studies of different wireless technologies for various power system applications still exist [3]. The main benefits of implementing wireless technologies compared to wired ones include reduced cabling, ease of maintenance, and rapid deployment.

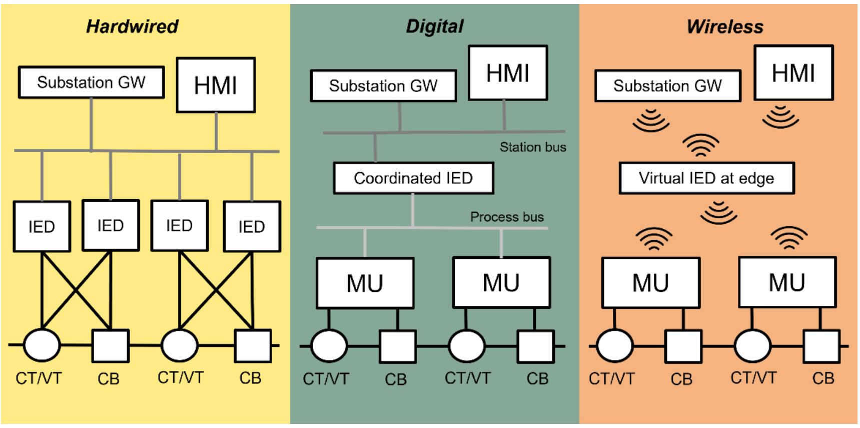


**Figure 1.** Substation automation architecture from hardwired to digital to wireless.

The main requirements for communication of power system applications are latency and reliability. Depending on the application, the requirements can be vastly different. Power system applications can be divided roughly into three segments based on the type of communication requirements: monitoring, control, and protection, as illustrated in Figure 2. Monitoring requires connection to a massive amount of devices with low bandwidth for each device. Latency and reliability should remain at a moderate level for monitoring. On the contrary, control applications require high reliability to ensure the timely delivery of control signals and lower latency than monitoring. The device density of the control application and the required bandwidth is lower. Protection applications have the ultimate service priority due to their critical role in stabilising the grid and limiting the damage in case of faults. Along with the high service priority, reliability requirements are ultrahigh, and latency requirements are extremely low. Protection applications' device density and bandwidth requirements are lower than control applications.

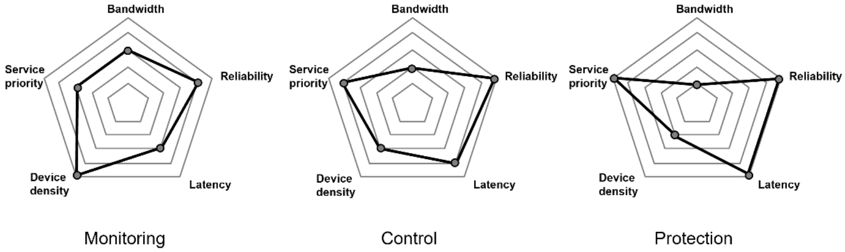


**Figure 2.** A high-level overview of power system communication requirements.

Since the communication requirements of monitoring and control applications are less strict than protection applications, prior wireless technologies such as fourth-generation cellular network (4G) could provide suitable communication network infrastructure. Similarly, for indoor applications, in households, wireless technologies such as Bluetooth or Zigbee could meet the needs of the communication infrastructure [3].

Prior wireless technologies have yet to achieve protection applications' reliability and latency requirements. The requirements are strict due to the time-critical nature of the protection applications. Limiting the damage to the grid infrastructure and danger to society in case of a fault can depend on operation of the protection in tens or hundreds of milliseconds. As the prior wireless technologies have not achieved the communication requirements of protection applications, now the question remains: Can the fifth-generation cellular network (5G), which was announced at its launch to reach 1 ms latency [4], achieve them?

## 1.2 Objectives and scope of the thesis

According to the promised targets of 5G, it seems, in theory, to be suitable for the communication of protection applications. However, it needs to be clarified. Does 5G meet all the initially promised targets in practice since its implementation and rollout are conducted in several phases to ensure smooth integration with the existing wireless network infrastructure and a sustainable investment cycle? Typically, studies on the applicability of wireless technologies for smart grid applications have been conducted via pure simulation or by integrating simulated wireless networks into a real-time simulation of power systems. This approach lacks the accuracy of commercially available wireless networks, which the industry would use as the communication channel. This is the main motivation for this thesis; thus, the main research question is whether commercially available 5G is applicable for protection communication. The following subresearch questions support this main research question:

- What prior bottlenecks does 5G remove regarding deployment for protection communication?
- What limitations does 5G have hindering its application on protection communication?
- How could the identified limitations of 5G be addressed in protection communication?

The focus of the thesis is communication in protection applications in medium voltage grids, with a special emphasis on three applications of line differential protection, intertrip protection, and fault indication. The scope is further narrowed to focus on International Electrotechnical Commission (IEC) 61850-based communication protocols of Generic Object Oriented Substation Event (GOOSE) and Sampled Value (SV) in the protection applications and usage of wireless 5G to transmit these protocols. In the case of line differential protection, the focus is on bidirectional routable SV communication between two protection IEDs and with intertrip protection on unidirectional trip command transmission routable GOOSE. The fault indication focuses on IEC 61850-9-2 SV and GOOSE transmitted via a virtual private network (VPN) connection. In all these cases, only the communication section in focus has been transmitted in a 5G network. Thus, the studies on the applicability of 5G for protection communication are limited to this section of the communication network. The thesis is limited to commercially available 5G networks in Finland and performance measurements of the telecommunication providers commercially available services in terms of wireless communication. While the power system part of the thesis is limited to controller-hardware-in-the-loop (CHIL) simulations in which hardware intelligent electronic devices (IEDs) and the 5G network form the system undergoing the test.

### 1.2.1 Contributions of the publications

The dissertation consists of seven publications holistically providing answers to the research questions of this thesis. The main content and contributions of these publications are summarised in this section.

Publication 1 describes the potential challenges and opportunities of implementing edge computing-supported smart grid protection applications. Fault indication is especially demonstrated to achieve decreased latency if edge computing is employed. The main contribution is the discussion about various aspects of edge computing in the context of protection applications. Publication 1 provides answers regarding edge computing on how 5G could remove prior bottlenecks while highlighting potential limitations. Edge computing decreasing overall latency in the transmission of SV measurement data is highlighted by a combination of CHIL simulation and computational study.

Publication 2 discusses edge computing and 5G standalone (SA) as a platform for smart grid applications. Suitable smart grid applications for edge computing with a special focus on protection applications are proposed. The pilot environment measurements compared the performance of 5G SA to non-standalone (NSA) for a fault indication. Publication 2 contributes to research questions on how 5G is improving compared to its predecessors and how the existing implementations of 5G are developing from NSA to SA. The discussion on suitable smart grid applications for edge computing also highlights the limitations of 5G edge in the context of smart grids.

Publication 3 proposes a methodology to decrease packet loss of IEC 61850-based communication in a 5G network by data compression. The methodology bundles data packets from several merging units horizontally and vertically to form larger data packets more suitable for the 5G network. One of the limitations of 5G for protection applications is that small packets typical for protection communication are not the optimal size for a 5G network leading to unnecessary packet loss and a decrease in reliability. Publication 3 contributes to the research question of how the limitations of 5G could be addressed.

Publication 4 demonstrates the impacts of cyberattacks on substation and grid automation. Two cyberattacks exploit the process bus communication and one affects the priority of time synchronisation communication. The cyber-attacks are based on IEC 61850 communication protocols. Publication 4 assesses the impacts of cyberattacks on the electrical grid. Similar consequences could be attained if the 5G network does not meet the reliability and latency communication requirements and causes operation failure of protection applications.

This answers the research question on the limitations of 5G for protection applications.

Publication 5 describes forensic methods that could be used to discover and analyse cyberattacks in substation and distribution grid environments. CHIL demonstrations with IEDs forming a part of a substation are deployed to capture digital IEC 61850 signal data and cyberattacks targeting it. Publication 5 highlights that IEC 61850-based communication protocols are not inherently cybersecure by design, as they have been originally designed to be deployed in private networks without external connectivity. It is crucial to consider cybersecurity when deploying IEC 61850-based communication in a public network. Without 5G providing cybersecurity solutions, the lack of consideration for them in IEC 61850 could limit the applicability of protection applications on 5G networks.

Publication 6 proposes a communication-free charge controller for electric vehicles according to a fairness mechanism among the charging points. The main contribution is to highlight communication networks' reliability and availability. Depending on the geographic location, service provider, and infrastructure available in the area, the reliability requirements of the application might not be met, such as in the case of this publication with electric vehicle (EV) charging control. The intelligent and optimised operation must be achieved by local optimisation without coordination via a communication network. Publication 6 provides a counterpoint to the main aim of the thesis.

Publication 7 validated two approaches to prioritise protection communication in the 5G network. Due to the lack of recommendations for prioritisation in wireless networks and the need for granularity of network slicing, further approaches are required to improve the reliability of protection communication. One of the approaches prioritises all incoming traffic to the network at the network switches, allocating the largest share of bandwidth for protection communication. In contrast, the other approach adjusts the amount of live video stream traffic in the network to provide a larger share of bandwidth for protection communication. Publication 7 contributes to research questions on the limitations of 5G and how the limitations could be addressed.

Contributions of the thesis based on publications and their novelty and methodology are presented in Figure 3.

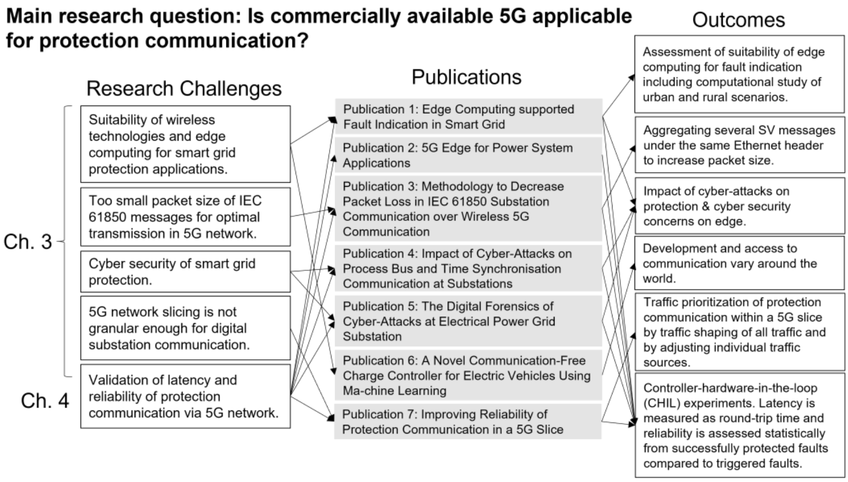

Main research question: Is commercially available 5G applicable for protection communication?
Research Challenges
Publications
Outcomes
Ch. 3
Ch. 4
Suitability of wireless technologies and edge computing for smart grid protection applications.
Too small packet size of IEC 61850 messages for optimal transmission in 5G network.
Cyber security of smart grid protection.
5G network slicing is not granular enough for digital substation communication.
Validation of latency and reliability of protection communication via 5G network.
Publication 1: Edge Computing supported Fault Indication in Smart Grid
Publication 2: 5G Edge for Power System Applications
Publication 3: Methodology to Decrease Packet Loss in IEC 61850 Substation Communication over Wireless 5G Communication
Publication 4: Impact of Cyber-Attacks on Process Bus and Time Synchronisation Communication at Substations
Publication 5: The Digital Forensics of Cyber-Attacks at Electrical Power Grid Substation
Publication 6: A Novel Communication-Free Charge Controller for Electric Vehicles Using Ma-chine Learning
Publication 7: Improving Reliability of Protection Communication in a 5G Slice
Assessment of suitability of edge computing for fault indication including computational study of urban and rural scenarios.
Aggregating several SV messages under the same Ethernet header to increase packet size.
Impact of cyber-attacks on protection & cyber security concerns on edge.
Development and access to communication vary around the world.
Traffic prioritization of protection communication within a 5G slice by traffic shaping of all traffic and by adjusting individual traffic sources.
Controller-hardware-in-the-loop (CHIL) experiments. Latency is measured as round-trip time and reliability is assessed statistically from successfully protected faults compared to triggered faults.

**Figure 3.** Contributions of the thesis based on publications, novelty, and methodology.

### 1.2.2 Structure of the thesis

The rest of the thesis is organised as follows. Chapter 2 provides an overview of IEC 61850-based protection communication and various protection applications with their communication requirements. Chapter 3 introduces 5G and its features, including network slicing, edge computing, and prior bottlenecks that 5G aims to remove. Chapter 4 summarises the CHIL studies and relevant results of the publications. Finally, Chapter 5 provides the conclusions of the thesis.

# 2. IEC 61850-based protection communication

This chapter discusses power system protection, relevant standards, and communication requirements for protection applications. Section 2.1 describes power system protection in general. Section 2.2 describes IEC 61850 and especially its communication protocols. IEC 61850 defines communication protocols for substation automation and is used in digitalised protection, especially in Europe. Protection applications are discussed in Section 2.3, which presents the communication requirements for selected protection applications.

## 2.1 Power system protection

Power system protection is the system that aims to detect faults in the electrical grid and limit the grid area and geographic area impacted by the fault. The main reasons to mitigate the impacts of faults in the grid are financial and societal aspects of safety and security. Faults can cause irreversible damage to the grid infrastructure and equipment connected to the grid, and repairing or replacing equipment can have enormous financial implications for the distribution system operator (DSO). Electrical grid operation regulations determine penalties for the number and duration of interruptions in electricity supply to customers. At the same time, if faulty grid components come in contact with humans or nature, people can get seriously injured, even suffering fatal injuries.

Protection is based on measuring selected grid parameters, such as voltage and current, and detecting anomalies and deviations in the measured values compared to the predefined operational range for each parameter. The measured parameters depend on the operated protection application. For instance, a simple overcurrent protection application requires current measurements from each phase. Protection follows five principles: reliability, stability, sensitivity, selectivity, and timeliness. Reliability means that the protection must always be operational, while stability means that protection must not react to the normal operation of the grid. Furthermore, protection must be sensitive enough to react even to minimal measurement changes. Protection must also disconnect only a minimal amount of the grid closest to the fault location and operate as fast as possible.

The protection system includes measurement devices interconnected to the grid and devices that provide protection functionality. Finally, these devices communicate the events in the protection to a control centre of the DSO for further action or reporting. In a modern, digitalised, protection environment, the measurements from the grid are captured by merging units and transmitted to IEDs as IEC 61850-based communication protocol SV as illustrated in Figure 1. IEDs house the protection functionality and can be located along the power lines in the grid or centralised at the substation, depending on the requirements of the protection application. The IEDs exchange data on the grid protection status via IEC 61850 GOOSE communication protocol. They can transmit events and reports to the control centre level via IEC 61850 Manufacturing Message Specification (MMS) communication protocol.

There are several protection applications, of which a subsection requires communication while others can offer enhanced functionality when a communication channel is deployed. These applications include differential, intertrip, and distance protection. Differential protection compares measurements from at least two measurement points and trips the breaker if there is a difference in these compared values. Intertrip protection sends trip commands from one IED to another, opening the corresponding breaker immediately. Distance protection compares the impedance calculated based on current and voltage measurements to a known line impedance; if the measured impedance is smaller than the known value, the trip command is sent to open the breaker. While distance protection does not inherently require a communication link, deploying one can increase its operational speed as a relay can communicate its status to relays close by, indicating a need for tripping or blocking. This thesis focuses on three protection applications implemented in the pilot environment: line differential protection, intertrip protection, and fault indication.

## 2.2 IEC 61850

IEC 61850 [5] is a substation automation standard commonly used at digital substations in Europe. The standard defines both data model and communication protocols for substation automation, which are separate. Thus, adding new data points and structures to the data model is possible without impacting the communication protocols. The data model and communication protocol devices are mapped using substation configuration language (SCL), which is also defined in IEC 61850. The mapping is based on extensible markup language (XML) over several configuration files with a specific hierarchy. The separation of the data model and communication protocols and the hierarchical configuration files enabling rapid additions of new devices to the system is seen as the main benefits of the standard, which IEC 61850 has expanded to encompass nearly the entire smart grid automation needs.

IEC 61850 defines three communication protocols: SV, GOOSE, and MMS. Each of the protocols has a slightly different target communication type. SV is meant to transmit measurement signals continuously on the process bus level. GOOSE is for transferring sporadic, event-based data between IEDs at the process bus and station bus levels. SV and GOOSE transfer time-critical data in a publisher-subscriber manner. MMS is a client-server-based protocol for station bus communication. MMS is mapped on all Open Systems Interconnection (OSI) stack layers, while SV and GOOSE are layer-two traffic [6]. IEDs, the core equipment in a protection system, use all three IEC 61850 communication protocols for exchanging data. This thesis focuses on SV and GOOSE communication via wireless 5G.

### 2.2.1 SV

IEC 61850-5 [7] defines specific requirements for the latency and reliability of SV messages. The communication requirements for SV messages are tightly related to the requirements for GOOSE communication as SV messages can be used as data sources for protection functions, which communicate via GOOSE. Within a substation and one bay, the SV message latency requirement is less than 3 ms for the total transmission time, and between bays or substations, the requirement is less than 10 ms [7]. The required bandwidth for SV messages is high, as one IED can generate approximately 5 Mbps of SV data to the network [8]. Reliability is defined in IEC 61850-5 based on transmitting unwanted commands and the missing transmission of wanted commands. Similar to total transmission time, SV message reliability follows GOOSE communication requirements. Thus, missing commands should only occur with a probability of $10^{-4}$ and transmission of unwanted commands with a probability of $10^{-8}$ [7]. As for SV communication's recovery time, only a few consecutive samples can be lost [7]. SV communication does not include acknowledgement messages by the receiver, but lost samples are overwritten by the next successfully transmitted sample [8]. Overall, it is far worse for SV messages to be excessively delayed than completely lost during transmission since the next arriving SV messages can replace the lost message.

### 2.2.2 GOOSE

Similar to SV communication, requirements for GOOSE communication are defined in IEC 61850-5 [7]. The total transmission time of GOOSE messages depends on the application. For trip messages within a substation and the same bay, the total transmission time is less than 3 ms, and within bays or substations, it is less than 10 ms [7]. For other fast messages, the total transmission time is less than 20 ms [7]. For communication between substations, several total transmission times are defined, ranging from 4 ms for trip signals to beyond 20 ms for normal state-based applications [9]. Therefore, the maximum delay of trip signals is 3 ms, and other GOOSE messages range from 10 ms to 100 ms [8]. The reliability requirements for GOOSE messages are the same as those introduced above for SV. The recovery time for GOOSE message-based applications is 8 ms, and for communication is 4 ms [7]. Similar to SV, GOOSE does not include acknowledgement messages by the receiver and thus has a retransmission system for the messages based on time intervals defined in IEC 61850-7-2 [10]. While the priority requirement for GOOSE messages is high in the case of trip commands, the required bandwidth is low as in steady-state, and one IED transmits approximately one Kbps of GOOSE traffic as a heartbeat signal, which increases as the state changes to a burst of messages approximately 1 Mbps [8].

## 2.3 Communication requirements of protection applications

Communication requirements of different protection applications depend on the type of communication required to operate the application. The simplest applications, which operate on just one IED, have operational time requirements that only depend on the internal operation of the IED. Differential protection applications require an exchange of measurement data between two locations in the grid. A bidirectional communication link between the IEDs is required to facilitate this measurement exchange. Intertrip protection requires a monodirectional communication link to transmit the trip signal from one IED to another. Communication link requirements of fault indication depend on the type of system implemented. For the fault indication in this thesis, the communication link requirement is bidirectional: uplink for transmitting measurement data and downlink for trip signals.

Each of the protection applications has its communication requirements, which are defined by various sources such as IEC 61850 [5] and International Council on Large Electric Systems (CIGRE) Technical Brochure (TB) 192 [11]. Also, depending on the country, protection systems are implemented according to different standards, the country's grid codes [12-14], and the technical instructions of grid operators [12]. The grid codes and technical instructions typically outline an overall fault clearance time within which the whole operational chain must occur, from detecting the fault to clearing it. Therefore, there can be drastic changes in the implementation and requirements of specific protection applications depending on the geographic location. To further increase the complexity of the communication requirements, the specific numerical values determined for parameters, such as latency, vary depending on the physical location of the protection equipment and their relational distance and location within the protection system. For instance, latency requirements can range from intrasubstation 3 ms to intersubstation 20 ms [9]. DSO-specific requirements for total operational time of protection, including the customer's network, can be 100 ms for medium voltage grids [12].

### 2.3.1 Line differential protection

Line differential protection operates by exchanging current measurements between two IEDs. If either of the IEDs independently detects a difference in the current measurements, they open the corresponding breaker. In this thesis, the current measurement exchange is transmitted using routable SV messages. Routable messages are Internet Protocol (IP) level traffic, thus not requiring tunnelling in the wireless network. The communication setup for line differential protection via 5G is depicted in Figure 4.

Communication requirements for this communication link are derived from IEC 61850 and its requirements for SV communication. The transfer time for

SV communication within a substation is less than 3 ms and outside a substation less than 10 ms [7]. Similarly, other requirements for SV messages are described in subsection 2.2.1. According to TB 192 [11], propagation time for line differential protection must be less than 10 ms, and jitter must be less than 10 ms [11]. The required bandwidth is typically 64 Kbps, while probability of operation loss should be less than $10^{-6}$ in normal situations and less than $10^{-5}$ in fault situations [11]. Furthermore, TB 192 recommends using a licensed radio link as a communication channel only if the communication channel delay remains under the relay's delay compensation adjustment range [11].

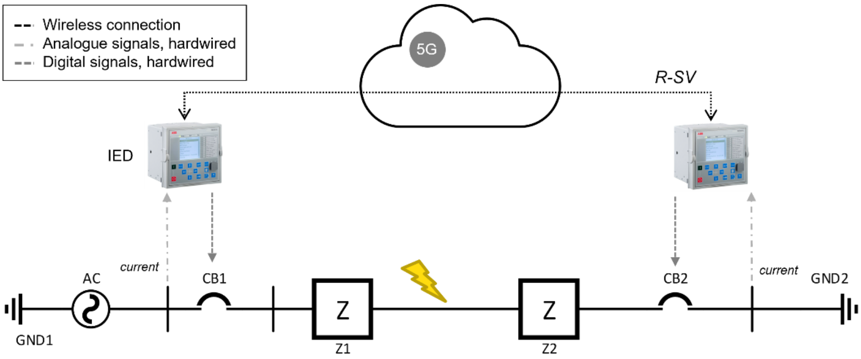


**Figure 4.** Line differential protection communication via 5G.

### 2.3.2 Intertrip protection

Intertrip protection communicates a trip command from one IED to another, opening the breaker immediately. In this thesis, the trip command is transmitted using a routable GOOSE message. The communication setup for intertrip protection via 5G is depicted in Figure 5. Compared to the setup of line differential protection in Figure 4, the intertrip protection uses the same physical IEDs, but one of the IEDs is triggered to transmit the trip command to the other IED, which opens the connected breaker.

Communication requirements for GOOSE messages are derived from IEC 61850-5. Within the substation, transfer time is less than 3 ms, and outside the substation, is less than 10 ms for trip commands [7]. Similarly, other requirements for GOOSE messages are described in subsection 2.2.2. According to TB 192 [11], propagation time is less than 30 ms for intertrip, while jitter and symmetry are not critical. Furthermore, the bandwidth requirement is low, less than ten Kbps, and probability of operation loss should be less than $10^{-5}$ in normal situations and less than $10^{-4}$ in fault situations [11]. The requirements for the missing trip and unwanted commands are higher for intertrip than line differential. Using a licensed radio link as a communication channel is acceptable for intertrip [11]. According to IEC 60834-1, total operating time excluding communication channel should remain at 10 ms, and the probability for unwanted commands is less than $10^{-8}$, while the probability for missing commands is less than $10^{-4}$ [13].

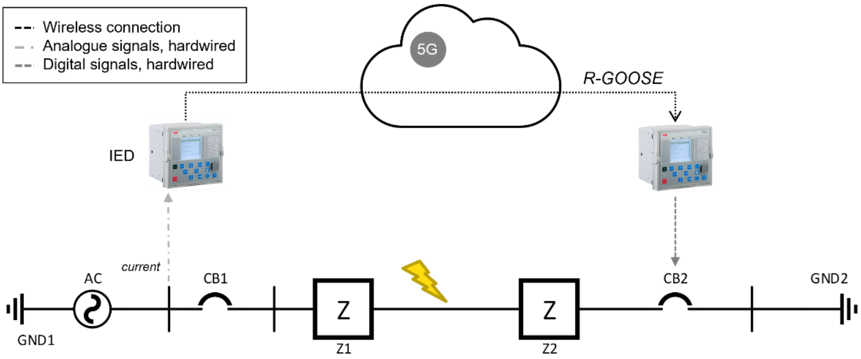


**Figure 5.** Intertrip protection communication via 5G.

### 2.3.3 Fault indication

Virtual fault passage indication is not directly a protection application, but a protection-related application in this thesis is operated by directional overcurrent protection. Current and voltage measurements are sampled by merging units and transmitted as SV messages to an edge device hosting the protection application. The edge device combines directional overcurrent protection results to assess which grid section the fault is located in. Once the grid section is known, the edge device sends trip commands as GOOSE communication via merging units to the appropriate breakers. In this case, both SV and GOOSE communication is transmitted in a VPN tunnel when in the wireless communication channel. The communication setup for fault indication via 5G is depicted in Figure 6. Unlike line differential and intertrip protection setups in Figures 4-5, merging units record SV streams of current and voltage, and the fault indication operates on the edge device.

Communication requirements for the fault indication can be derived from SV and GOOSE communication requirements in IEC 61850. For GOOSE communication, the transfer time must be less than 10 ms outside a substation and less than 3 ms within a substation, which is also applied to the SV messages [7]. SV communication requires high bandwidth and priority and can sustain a few lost samples [8]. The probability for missing commands is $10^{-3}$ and $10^{-4}$ for unwanted commands [13].

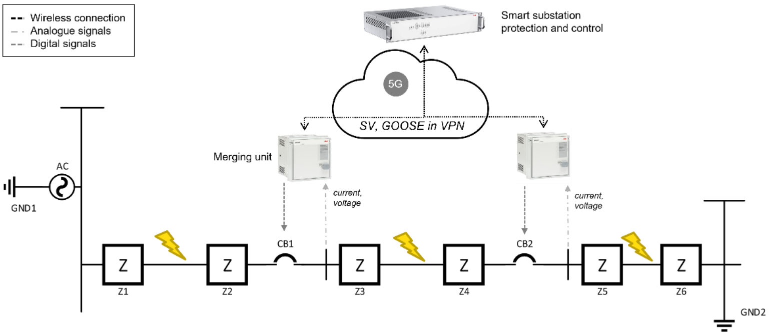


**Figure 6.** Fault indication communication via 5G.

# 3. Protection communication via 5G

This chapter introduces 5G and its key concepts in Section 3.1. Section 3.2 describes what 5G could provide for protection communication. Section 3.3 responds to one of the subresearch questions of this thesis by discussing the challenges that remain with 5G. Finally, Section 3.4 outlines possible solutions to combat challenges when applying 5G for protection.

## 3.1 5G introduction

This section explains the key concepts of 5G, including NSA and SA, network slicing, edge computing, and Ultra-Reliable Low Latency Communication (URLLC). Moreover, 5G targets at launch are highlighted, and the prevalence of 5G deployments worldwide is mentioned.

### 3.1.1 5G non-standalone and standalone

5G is cellular technology developed between 4G Long Term Evolution (LTE) and 5G-Advanced/6G. It employs a higher frequency range than its predecessor, reaching a millimetre wave frequency band on the electromagnetic spectrum. More data can be sent simultaneously with higher frequency, but the distance the data can reach before fading becomes shorter. Thus, 5G deploys small cell base stations in the mmWave range, which cover smaller geographic areas with higher density.

5G is not deployed in a vacuum but must integrate into legacy cellular networks smoothly. Various deployments have been suggested [14], and they can be divided into non-standalone and standalone solutions. NSA means that the 5G radio access network (RAN) is integrated into the 4G core enabling early deployments on top of existing 4G LTE infrastructure while the 5G infrastructure investments are ramping up. Therefore, NSA only includes some of the features and performance capabilities of 5G targets. SA is a fully 5G-based solution with a 5G RAN and core.

### 3.1.2 Network slicing

5G introduces network slicing, which enables dividing 5G RAN into independent slices. Each slice has its parametrisation for the communication channel, and adjacent slices can be optimised for different types of signal transmission without disturbing one another. The idea is to offer options for end users who might not have the capacity or business case to purchase entire wireless networks but could subscribe to a slice of the existing 5G network. Network slicing can be more cost-effective, especially if the end user would have been required to invest in ICT infrastructure for the whole network. The end user of the slice can decide, with the support of the telecommunication operator, the type of services and optimisation to be deployed on the slice.

### 3.1.3 Edge computing

Apart from network slicing, 5G also brings edge computing to the forefront. Edge computing is not a new concept, but rather further development of cloud computing. While cloud computing shifted operations from the network or physical locations close to the sensors to the cloud, edge computing brings the computing power for operations to the network's edge from the core. If edge computing is used, all the signals do not need to be transmitted to the network's core, but only to the edge, decreasing the signal transmission time. There could also be a separation between the data that is processed locally, at the edge, and in the cloud to decrease the amount of data sent to the cloud that requires specialised hardware for preprocessing at the physical location of the sensor. In the context of this thesis, the edge is assumed to be located at a 5G base station.

### 3.1.4 5G use cases

5G emphasises more industrial applications than the consumer cell phone market compared to prior cellular networks. Therefore, three main use cases have been defined for 5G to support industrial end users in identifying their requirements. These use cases are associated with a service portfolio optimised for the specific needs of each of the use cases. The use cases are enhanced Mobile Broadband (eMBB), URLLC, and massive Machine Type Communication (mMTC). eMBB service selection is focused on control applications, which require medium latency and bandwidth compared to URLLC and mMTC. URLLC targets time-critical applications offering low latency and high reliability. mMTC serves mostly Internet of Things (IoT) and monitoring applications, which have massive amounts of sensors or data collection points in the system transmitting data to a centralised location such as the cloud. The characteristics of each use case are illustrated in Figure 7. The use cases are employed together with network slicing, and the end user can select a service portfolio associated with one of the use cases for their slice.

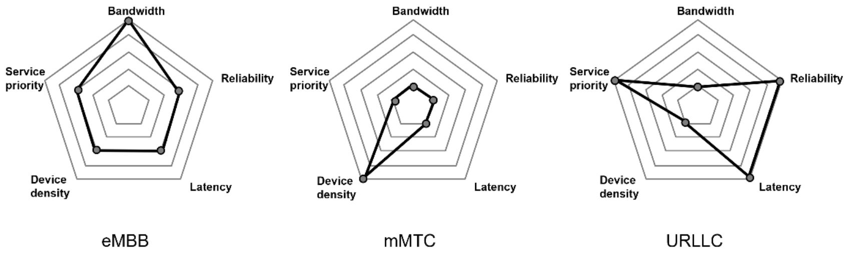
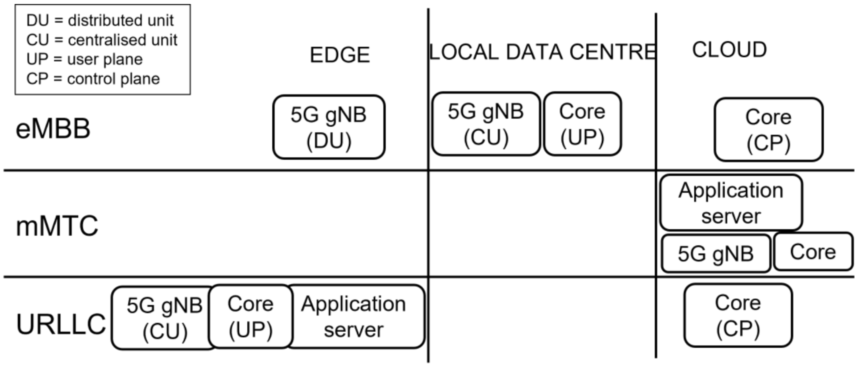


**Figure 7.** 5G use case characteristics adapted from [15].

The 5G use cases achieve the different characteristics by allocating components of the RAN and core to different locations ranging from edge via local data centres to the cloud. Depending on how far the application is operated determines the expected latency. For instance, mMTC use case operations are concentrated in the cloud and URLLC on the edge. The allocations are depicted in Figure 8.


DU = distributed unit
CU = centralised unit
UP = user plane
CP = control plane

| | EDGE | LOCAL DATA CENTRE | CLOUD |
|---|---|---|---|
| eMBB | 5G gNB (DU) | 5G gNB (CU)<br>Core (UP) | Core (CP) |
| mMTC | | | Application server<br>5G gNB<br>Core |
| URLLC | 5G gNB (CU)<br>Core (UP)<br>Application server | | Core (CP) |

**Figure 8.** Allocation of 5G components mapped to the edge, local data centre, and cloud adapted from [16].

### 3.1.5 5G promises at launch

At its launch, several ambitious targets were announced for 5G. Like all prior cellular networks, 5G also promised faster download speeds than 4G LTE - up to 10 Gbps [4]. Furthermore, 5G was the first cellular technology to specifically target industrial applications and end users rather than consumer cell phones. To enable industrial applications, many of which had previously used wired connectivity, 5G promised 1 ms latency [4]. 5G also aims to support the connectivity of a massive number of devices, enabling extensive deployments of IoT solutions.

### 3.1.6 5G deployment in the world

5G was launched by the 3rd Generation Partnership Project (3GPP), with the first release of standardisation of the technology in 2017. Since then, telecommunication operators have been investing in various deployments. According to the Global mobile Suppliers Association (GSA), by the end of March 2023, 40%

of countries and territories globally have deployed 5G access and 46% of telecommunication operators that have deployed 5G are investing or deploying 5G SA [17]. Compared to the telecommunication operators, which have commercially launched 4G LTE, only 14% are investing or deploying 5G SA by the end of March 2023 [17].

## 3.2 5G-supported protection communication

While 4G LTE is suitable for most smart grid applications using communication [3], most protection applications have communication requirements that 4G LTE does not meet. Due to the 5G targets announced at its launch, especially 1 ms latency and URLLC use case and associated service portfolio, 5G is a potential technology to meet the requirements of protection applications.

This section highlights the benefits of using 5G for protection communication from the perspective of 5G SA, network slicing, edge computing, and 5G use cases, especially URLLC, based on the introduction in Section 3.1.

### 3.2.1 5G SA

5G SA improves the latency and reliability of cellular networks compared to 5G NSA and 4G LTE. Latency decreases from 4G LTE to 5G SA by tens of milliseconds. These latency and reliability limitations have been the main challenges with using prior cellular technologies for protection communication. Most protection applications require a latency of a few milliseconds combined with ultrahigh reliability. Typically, even if wireless technologies have met the latency requirement, they have occasionally lacked reliability and vice versa. Thus, 5G SA creates an intriguing opportunity as the deployment of 5G is capable of meeting the millisecond range latency requirements.

### 3.2.2 Network slicing

Traditionally, if utilities have used wireless technologies, they have built private networks, which require large investments and skills in the operation of communication networks. 5G, with all its services and features, requires increased knowledge of communication networks. At the same time, investing heavily in new wireless networks each decade can overwhelm the budget of a utility when the typical lifecycles of grid components can be 25 to 40 years or more. Network slicing allows utilities to subscribe to an optimised slice selection for their operations and defines the telecommunication operator service requirements for each slice.

Protection communication and substation automation have various types of communication traffic with highly heterogenous communication requirements. Thus, network slicing offers a standard way for utilities to define specific slices for each communication type, such as IEC 61850-based MMS, GOOSE, and SV traffic. Slicing allows the optimisation of highly granular slices for each substation communication traffic type rather than optimising only one type of communication traffic in the utility's network and hindering the transmission of other types.

### 3.2.3 Edge computing

Edge computing and its capability to decrease latency compared to cloud computing are highly relevant for protection communication. Moreover, edge computing releases protection functionality from its hardware confines located next to the sensors in the grid to a virtualised software running on the edge. With the decreased latency and computation location at the edge nearer to the physical equipment, it is possible to reimagine protection functionality and architecture that is not limited to individual physical devices.

Publication 1 highlights that the virtualisation of grid applications is not new but has already been proposed with cloud computing [18]. The concept has gained support due to edge computing, and several applications have been suggested to be implemented on edge, although less time critical than protection, such as condition monitoring [19, 20], surveillance [21], and smart metering [22]. Furthermore, fault detection at the edge has been proposed for transmission grids [19, 20, 23], but not for medium voltage distribution grids which is the focus of this thesis. Publication 2 outlines that suitable protection applications for edge could begin with applications requiring communication, such as permissive and blocking distance protection, intertrip, and differential protection. Suitable protection applications could also be assessed holistically, allocating backup protection to be coordinated from the edge. Further details of the benefits are discussed in Publication 1.

### 3.2.4 5G use cases: URLLC

Each service portfolio is relevant for smart grid applications: eMBB for control, mMTC for monitoring, and URLLC for protection applications, illustrated in Figure 9. Of the 5G use cases and associated service portfolios, URLLC is the most prominent for protection applications due to its requirements of low latency combined with high reliability. Low latency is needed to transmit the protection data within an adequate time, according to IEC 61850. While high reliability is crucial since a fault can occur at any moment, the network must always be available. For instance, in the event of a fault, an IEC 61850 GOOSE message is sent to trip a breaker; since GOOSE protocol does not include a return confirmation message, lack of reliability could prevent the trip signal from reaching the receiver.

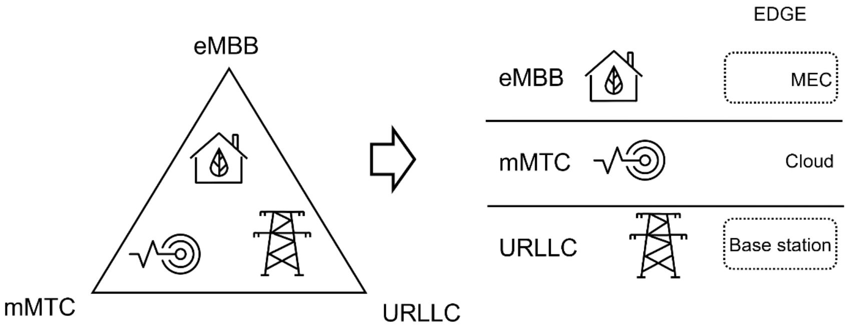


**Figure 9.** 5G use cases with associated power systems applications.

## 3.3 Challenges with 5G-supported protection

Sections 3.1 and 3.2 described the promises, targets, and benefits of 5G for protection communication. However, 5G has not developed without its challenges, especially in practice, which is the focus of this thesis. This section explains the challenges with 5G as a communication medium for protection.

### 3.3.1 Optimisation of packet size

In previous measurement campaigns of commercial 5G networks [14], one of the challenges that has appeared is the optimisation of packet size for the communication network. IEC 61850-based GOOSE and SV packets appear to be too small compared to the assumed optimal packet size for a 5G network. This disparity could be due to 5G, in general, targeting high-definition video live streaming applications, which incur large packet sizes, thus 5G is optimised for large packet sizes. A consequence of small packet size can be increased processing since there are relatively more packets, but each packet contains very little information. This processing of small packets might cause packet loss at the networking devices. Publication 3 outlines that increasing processing events increases the probability of packet loss.

Standards such as IEC 61869-9 recognise the small packet size of SV traffic and include approaches to combine several consecutive measurement samples in the same packet. However, it is impossible to indefinitely combine measurement samples into the same packet as overly long delays or intervals between the received SV packets by an IED can impact the operation and accuracy of protection functions. Faults in the power system also include minor events that do not require interrupting the power supply, such as a small tree branch falling on overhead lines. Thus, a too-long delay in receiving the next measurement samples can cause incorrect operations that interrupt the power supply when unnecessary or forgo interruption when necessary.

### 3.3.2 Network slicing granularity

While the initial concept of network slicing is suitable for the heterogenous communication traffic of protection systems and substation automation, its applicability relies heavily on the extreme granularity of the slices. Each communication traffic type at the substation should be allocated its own slice and services specifically optimised for it. Network slicing with adequate granularity for protection communication could be based on IEC 61850 communication protocols as separate slices.

This granular slicing might have been the aim of the launch of 5G and network slicing. Still, based on 5G development and deployment, most telecommunication operators will have the capacity to offer one slice per vertical or end user rather than several slices [24, 25]. Therefore, network slicing might lack the granularity protection applications require and be suboptimised for only some communication traffic types in the slice. If other traffic is on the same slice as the protection communication, delays and packet loss might increase [26].

### 3.3.3 Edge computing concerns

Edge computing is highly interesting for protection systems as it allows novel functionalities and improved predictive maintenance. At the same time, edge computing increases the protection system's complexity and collaboration with the telecommunication provider. Since the edge computing concept is still developing, Publication 1 describes in detail several aspects utilities need to consider when assessing the applicability of edge computing, which are summarised in the following.

Edge computing can involve a utility deploying the applications on edge at the premises of the telecommunication operator either as software running on a server provided by the telecommunication operator or as hardware installed on the premises. In either software or hardware, accessibility should be included in the service level agreement (SLA) between the utility and the telecommunication operator. An accurate and reliable time synchronisation signal is crucial for the utility, and its importance increases if the measurement sampling and protection functionality are operated on different devices. A clock could already be available on the edge for the other operations, and a time synchronisation signal could be derived from there. However, suppose the accuracy of the origin source or used time synchronisation signal profile fails to meet the utility's requirements. In that case, edge computing's profitability diminishes as the utility must bring its clock to the edge.

Latency can remain a challenge; while the edge is closer to the end user than the cloud, it might still take subseconds to a second for a computation depending on the application and infrastructure. Thus, edge computing could only work for applications with second-scale latency requirements, such as anti-islanding protection, and not for line differential protection. Some low-latency applications might be implemented in the cloud, especially if they are intended for global optimisation. On the other hand, transmitting unnecessary data to the cloud should be avoided and instead preprocessed at the edge. Data reduction might not be possible for all power system measurements, such as phase angles, but some compression methods are discussed and presented in Publication 3.

A crucial part of the SLA is quality of service (QoS) monitoring and agreement on actions to be taken if the SLA's limits cannot be upheld. For utilities, historic QoS monitoring is not relevant, but real-time or predictive monitoring is. Another relevant part of SLA is maintenance, as a utility's expenses can increase if it must do regular maintenance at the edge sites in addition to their grid assets. The maintenance can be outsourced to the telecommunication operator if generic hardware is used for the applications. Virtualisation of protection applications could decrease the physical visits at the edge and enable hot-swapping of the application during maintenance or for redundancy.

The last crucial aspect is the implementation of security at the edge. Protection applications as part of operational technology (OT) networks can be vulnerable to cyberattacks, and their normal functionality can be used for malicious means. Consequences of cyberattacks on the power grid can be severe, as described in Publication 4, and difficult to detect with an insignificant increase in traffic, as described in Publication 5. Thus, edge should include defence mechanisms against cyberattacks without requiring an extensive increase to the computational capacity that increases latency.

### 3.3.4 5G deployments around the world

5G deployments are at varying degrees around the world. This dilemma adds additional complexity to the application of 5G for protection communication. In countries that have already implemented 5G, 5G SA networks are available with URLLC and edge computing services. Thus, protection applications can be implemented using 5G. Countries that lag behind in their 5G investment and implementation are also hindered in the use of 5G for protection communication. Therefore, it is crucial to consider which applications are implemented on edge and which on physical equipment while also integrating selectivity and redundancy to this assessment as explained in Publication 1. Applications operating on physical devices without communication requirements are equally important for manufacturers to keep in their product catalogues since communication network infrastructure could be limited depending on the country of implementation. Publication 6 provides an example of a noncommunication-based EV charging control algorithm receiving the relevant information for voltage and sensitivity analyses from the local measurements at the EV charging station due to a lack of reliable communication infrastructure.

## 3.4 Solutions to 5G challenges

Section 3.4 will suggest some solutions and considerations to the challenges of applying 5G on protection communication outlined in the previous section. All the presented solutions and considerations aim to enable utilities to use 5G for protection communication when suitable.

### 3.4.1 Packet aggregation

This subsection describes approaches to aggregate SV message packets to increase packet size to be more optimal for 5G networks based on prior literature and the proposed method from Publication 3.

*Related literature*
SV message compression has been addressed by IEC 61869-9 that defines standard sampling rates for compressing consecutive SV measurement samples. The standard compression for protection applications is two consecutive samples in the same Ethernet frame, which increases the latency of the first sample compared to the second sample in the frame. In [27], SV packets are compressed even more than in IEC 61869-9 by removing redundant data associated with each sample and only including this information in the aggregated packet. In [28], measurement samples are suggested to be transmitted as periodic GOOSE messages. Both approaches require knowledge of substation automation standards, which ICT engineers might not have. Typically, GOOSE messages are used to indicate sporadic events in the system, such as faults; thus, changing the nature of GOOSE messages to periodic might increase delays in response to faults. Publications 4-5 describe how GOOSE messages can be manipulated in a false data injection attack, which can be difficult to detect due to a lack of changes in the overall traffic at a substation. Implementing all process bus communication with GOOSE exposes more data and functionalities to these attacks.

*Proposed methodology*
This data aggregation approach does not format the data within the SV packets but focuses instead on the Ethernet headers of the packets. By aggregating a larger amount of data under the same Ethernet header, the packets transmitted in the wireless channel are larger, thus decreasing packet loss and requiring less bandwidth. The aggregated packet has TLV (Type, Length, Value) headers consisting of the information from the original packets, including the number of original packets, destination, source Media Access Control (MAC) address and indexes, and payload.

Since the SV packets are not reformatted, this approach can be used for horizontal and vertical data aggregation. Horizontal aggregation takes packets from multiple merging units or IEDs to be aggregated, and vertical aggregation compresses several consecutive packets under the same Ethernet header, similar to IEC 61869-9. The aggregation is implemented at the networking devices, and therefore is only operational when the packets are in the wireless network.

### 3.4.2 Traffic prioritisation in a slice

This subsection explains methods to prioritise protection communication traffic at a substation based on prior literature and the proposed method from Publication 7.

*Related literature*

Prioritisation of critical traffic flows has been recommended in IEC 61850-90-4 [8], but as the recommended techniques are for wired connectivity, they are not appropriate for wireless networks. Many techniques, including Hierarchical Token Bucket (HTB), have existed for decades and are now experiencing a renaissance thanks to the ultrahigh reliability requirements of URLLC [29]. Prior approaches to prioritise smart grid communication suggested solutions for Cognitive Radio-based communication a decade ago [30-32]. Many prior prioritisation methodologies do not assign the highest priority to protection communication, but instead assign priority to smart meters [32] or lump protection communication together with all substation automation [30, 31]. Since then, scheduling algorithms for prioritisation have been proposed for LTE [33] and URLLC [34]. However, they fail due to a lack of insight into smart grids assigning the highest priority to demand response [33] and idealistically assuming each neighbourhood would include services ranging from Supervisory Control And Data Acquisition (SCADA) to load control and video surveillance [34].

Prioritisation can also be studied from the perspective of individual traffic sources, such as video streaming for surveillance, thermal imaging, or image processing-based detection at substations. In [35], adjusting the bit rate of the encoder output is proposed for video monitoring at the substation, but since the study was conducted over two decades ago, its focus was fibre networks. Furthermore, the lack of realistic communication traffic types limits [35] as only two traffic types of a video stream and alarms are considered. Conversely, [36] proposes an event-based video stream triggered by GOOSE messages. However, similar to packet size optimisation by switching to GOOSE from SV, exposing GOOSE communication to video streaming can expose process bus communication to cyberattacks, as described in Publication 4.

*Proposed methodology*

The proposed methodology attacks prioritisation from two angles: prioritising all traffic and dynamically adjusting individual traffic sources. The challenge of the prioritisation is to optimise the use of limited bandwidth while granting the highest priority to protection communication. Therefore, the overall prioritisation of all traffic is given by

$$B = x_1 f_1 + x_2 f_2 + \cdots + x_n f_n \tag{3.1}$$

subject to

$$B = 1 \tag{3.2}$$

$$1 \geq x_1 \geq x_2 \geq \cdots \geq x_n \geq 0 \tag{3.3}$$

where $B$ is bandwidth capacity, $x$ is priority indication as a weight, and $f$ is the amount of traffic per traffic type. Since the prioritisation targets industrial applications, it is appropriate to rank the traffic flows based on their priority leading to potentially dropping all of the least prioritised traffic.

The other angle to prioritisation is to adjust individual traffic sources, which can be given by

$$f_{source} = B - C_T \tag{3.4}$$

subject to

$$f_{source\_min} \leq f_{source} \leq f_{source\_max} \tag{3.5}$$

where $C_T$ is the total unavailable bandwidth at the moment $T$. As a result of (3.4), traffic generated by individual traffic sources is inversely correlated with unavailable bandwidth. Prioritisation according to (3.1) and (3.4) can be combined by

$$B = x_1 f_1 + x_2 f_2 + \cdots + x_n (B - C_T) \tag{3.6}$$

In this case, (3.6) assumes that only the last traffic source can be individually controlled, while the rest of the traffic types are prioritised by (3.1). Practical implementations of the proposed methodology using HTB [37] and uplink bit rate adaptation of live video stream are further described in Publication 7.

### 3.4.3 Computational edge scenarios

To assess the circumstances and suitability of edge computing for fault indication, Publication 1 includes a computational study of two edge computing scenarios in urban and rural settings. Parameters for each scenario are derived from public information on distribution grids in Finland and are presented in Table 1. The assessment focuses on two key performance indicators (KPIs) of total uplink traffic rate and a minimum number of edge devices required to process the measurement data from merging units.

**Table 1.** Computation edge scenario parameters.

| Case | Network length [km] | Number of feeder lines at a substation (average) | Number of secondary substations per feeder line (average) | Number of substations | Number of secondary substations |
|---|---|---|---|---|---|
| Rural | 2000 | 6 | 6 | 8 | 1226 |
| Urban | 6400 | 8 | 8 | 25 | 1983 |

The number of merging units was derived from the parameters in Publication 1 by

$$n_{MU} = n_{PS} \times [n_{FL} + n_{FL} \times 2 \times n_{SS}] \tag{3.7}$$

where $n_{MU}$ is the number of merging units, $n_{PS}$ number of primary substations, $n_{FL}$ number of feeder lines at a substation on average, and $n_{SS}$ number of secondary substations. According to the commercial merging units [38], the uplink traffic rate for a merging unit is set at 4 Mbps and downlink at 24 Kbps. Therefore, the total uplink traffic rate for the edge scenarios is derived from (3.7) by

$$r_{total\_UP} = n_{MU} \times r_{UPpMU} \tag{3.8}$$

where $r_{total\_UP}$ is the total uplink traffic rate, and $r_{UPpMU}$ is the uplink traffic rate per merging unit. Moreover, each edge device is assumed to process data traffic from 20 merging units [39]. Based on this result, the minimum number of edge devices is derived from (3.7) by

$$n_{ED\_min} = \left\lceil \frac{n_{MU}}{20} \right\rceil \tag{3.9}$$

where $n_{ED\_min}$ is the minimum number of edge devices required to process the data from the merging units. Based on (3.7-3.9), a step function was formed to indicate the total uplink traffic rate to the number of merging units. The results of the computational study are presented in Table 2.

**Table 2.** Computational study results for rural and urban edge scenarios.

| **Case** | **Number of merging units** | **Total uplink traffic rate [Gbps]** | **Minimum number of edge devices** |
|---|---|---|---|
| Rural | 624 | 2.5 | 32 |
| Urban | 3400 | 13.6 | 170 |

Depending on the scenario, different aspects arise as the KPI for the profitability of virtualising fault indication to a device located at the edge. For the urban scenario, the total uplink traffic rate is the KPI since a humongous amount of traffic requires equal processing capacity at the edge, especially when services such as redundancy and offloading are included. For the rural scenario, the small number of merging units is the main KPI leading to a lack of density and nonprofitability. In the rural setting, a solution could be sharing edge computing resources among several end users. Even then, if geographic distances between the merging units and edge are too great, increased latency could hinder edge computing-based operations.

# 4. Hardware-in-the-loop studies and discussion

This chapter summarises the results of the CHIL studies and discusses the main observations from the publications. This chapter aims to present the outcomes of the publications holistically rather than going through individual simulation results separate from the big picture. Section 4.1 describes the CHIL methodology, including prior implementations of similar methodologies. Section 4.2 summarises the results of the CHIL studies. Section 4.3 discusses the applicability of 5G as a communication medium for protection applications, which is the main research question of this thesis.

## 4.1 CHIL methodology

This section describes the CHIL methodology used in Publications 1-5 and 7 and related prior literature. CHIL is a subcategory of hardware-in-the-loop (HIL), in which the hardware connected to the simulation is a control device.

### 4.1.1 Related literature

The power system and communication network cosimulation concept is well established and aims to uncover codependencies between the two systems. Moreover, cosimulation in [26, 40-50] has studied protection applications using communication infrastructure. Various wireless technologies have been explored for protection applications, including CR [40], Wireless Local Area Network (WLAN) [41], custom channel [42], LTE [43, 44], Zigbee [45], WiFi [46, 47], and global system for mobile communications (GSM) [48]. [26, 49] have implemented a testbench with ABB RED670 IEDs for GOOSE and SV communication testing but do not mention the communication technology used in detail. Specifically, 5G networks have been studied related to GOOSE and SV communication [50, 51] and to routable GOOSE communication for logic selectivity and loss-of-mains protection [52]. However, none of [50-52] use hardware IEDs, but instead use software implementations. Furthermore, [50, 51] used simulated 5G networks [50] and prototype implementation of 5G core networks [51], which do not accurately portray the performance and development status of commercial 5G networks.

### 4.1.2 Methodology

The CHIL methodology studied the latency and reliability of three selected protection applications: line differential protection, intertrip protection, and fault passage indication. Latency was measured as the round loop time of the full CHIL operational chain from measurements to protection operation notification. Reliability was studied statistically based on successful protection operations to faults triggered. Simplistic grid models were simulated on the real-time simulation providing the power system to the CHIL. The system under test (SuT) consisted of medium voltage grid protection devices exchanging data through commercial 5G networks operated by mobile network operators in Finland. Commercial 5G networks were used in the implementation since they provide a realistic picture of the existing and developing 5G networks compared to pure simulation. A detailed description of the experimental setup is described in Publications 1-3 and 7. The CHIL setup is depicted in Figures 10-12.

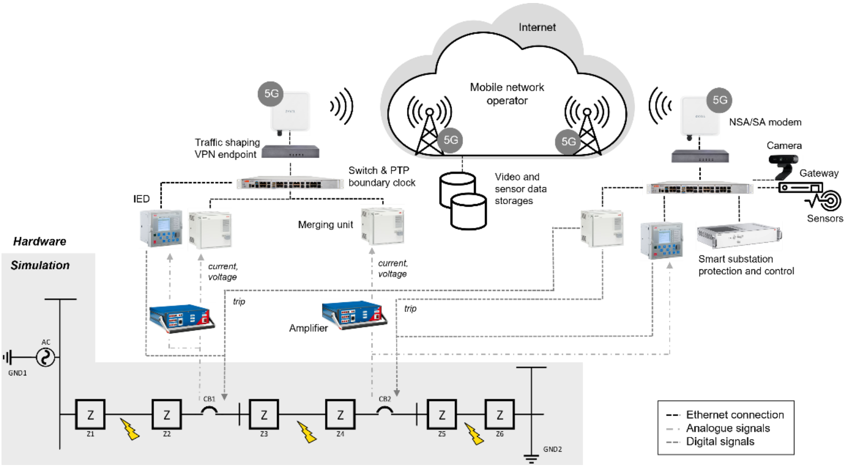


**Figure 10.** CHIL experimental setup.

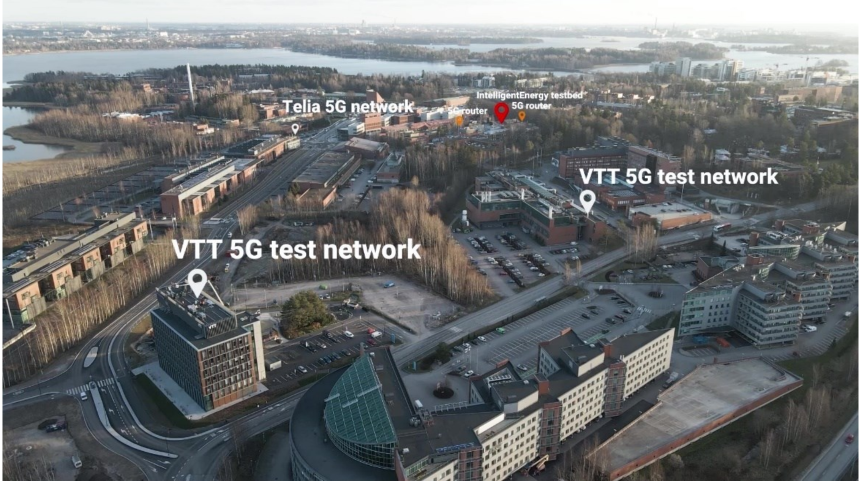


**Figure 11.** 5G networks in the system under test in Otaniemi, Espoo, Finland [53].

**Figure 12.** IEDs and merging units in the system under test at VTT IntelligentEnergy testbed [53].

## 4.2 Summary of the CHIL results

This section summarises the results of the CHIL studies. The results are addressed in terms of latency and reliability.

There is a huge disparity between 5G NSA and 5G SA, and it is apparent that using a fully-fledged 5G network (SA) significantly improves reliability and latency. In Figure 13, a drastic decrease in the successful operations of the protection can be seen for 5G NSA when the SV delay parameter controlling the buffer size at the receiver of the edge device is set to the default value of 100% [54]. On the contrary, in the SA network, 99.9958% of the faults are successfully protected, meaning the edge device received the SV messages from the merging units within the appropriate time frame, and there was no significant packet loss either. Thus, regarding reliability, 5G SA could be used for fault passage indication type of applications. Similarly, for latency, when round-trip times in NSA and SA networks are compared, the spread of round-trip times in Figure 14 for NSA is larger than in Figure 15 for SA. While absolute numbers of round-trip times cannot be directly compared due to different SV delay values, overall the round-trip time in SA networks tends to lean towards the shorter times and remain in the same range as the latency requirements for outside a substation.

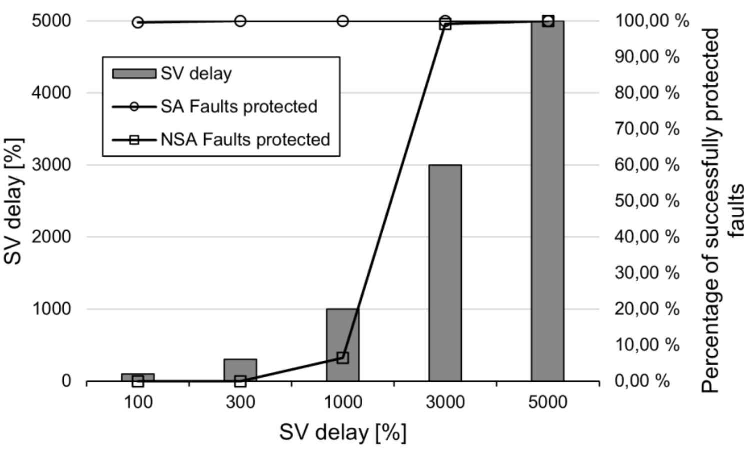


**Figure 13.** Percentage of successfully protected faults in NSA and SA compared to SV delay.

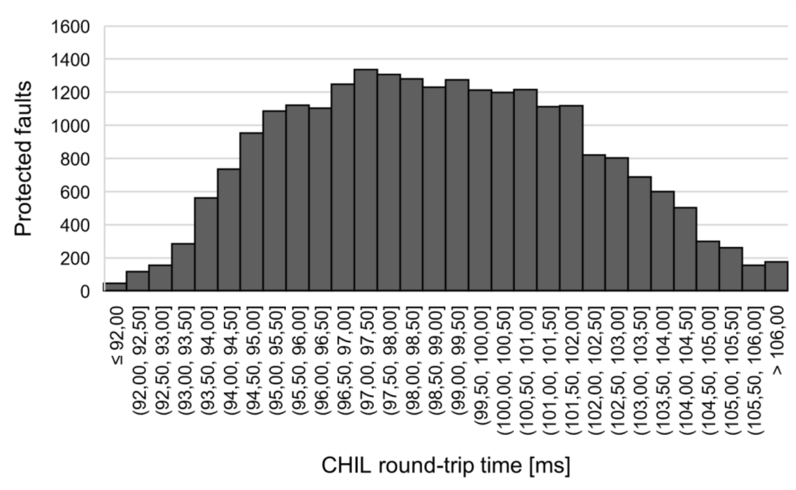


**Figure 14.** Histogram of round-trip times [ms] to protected faults in NSA.

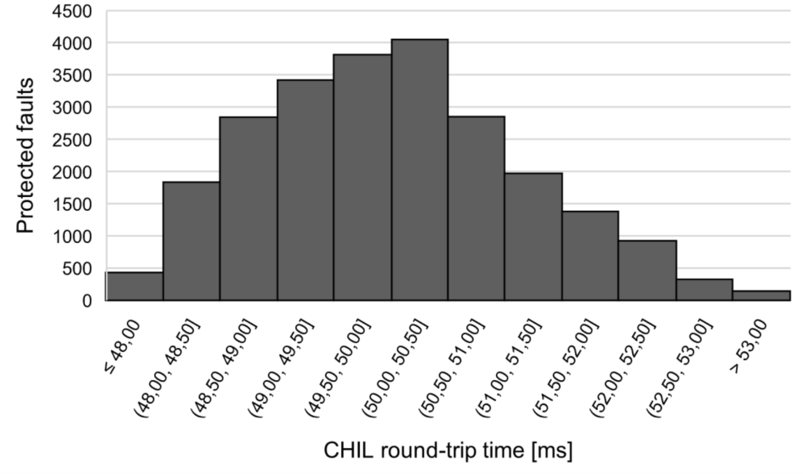


**Figure 15.** Histogram of round-trip times [ms] to protected faults in SA.

The application studied in Figures 13-15 is a virtual fault passage indication in which the directional overcurrent protection is operated on an edge device in the local 5G network. In terms of reliability, virtualising applications in separate edge devices in a SA network is satisfactory. However, depending on the geographic locations and distance, latency could increase beyond an appropriate level. In the case of Figure 15, the round-trip times are at a level in which the applications remain operational.

Prioritising overall traffic flows and live video streaming as an individual traffic source improves reliability but has no impact on latency based on the results. In Figure 16, when overall prioritisation (HTB) is used, the percentage of successfully protected faults remains at a similar level between 99.5–100%. Without prioritisation, the percentage of successfully protected faults decreases when more traffic is added to the network, as indicated by the four test cases in Figure 16. On the contrary, prioritisation does not impact latency; as seen in Figure 17, the histograms of prioritised and non-prioritised round-trip times remain at the same frequencies.

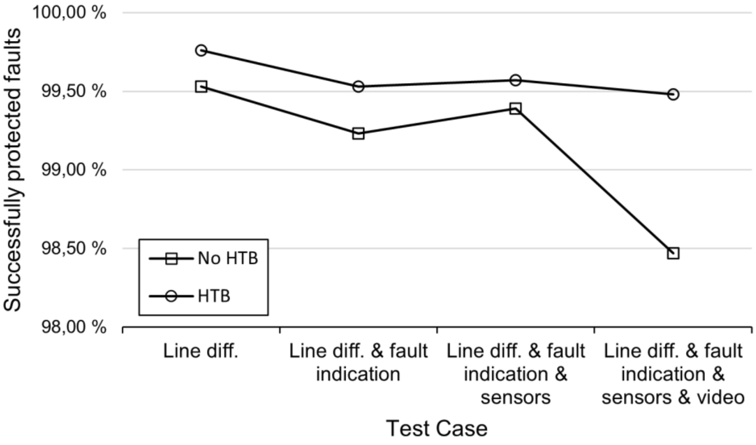


**Figure 16.** Percentage of successfully protected faults with and without HTB at various loads.

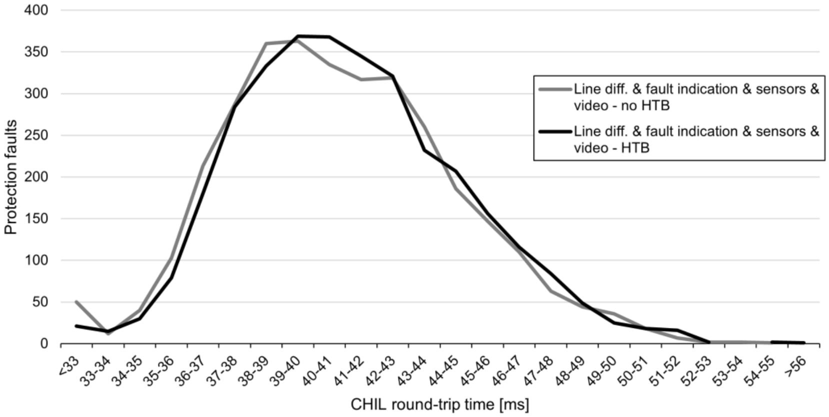


**Figure 17.** Histogram of round-trip times [ms] to protected faults with and without HTB.

The impact of individual traffic source control for prioritisation is the same regarding latency. In Figure 18, the round-trip times remain at similar levels irrespective of the change in video traffic in the network. On the other hand, reliability is drastically impacted, as illustrated in Figure 19. Without the HTB prioritisation lowering the amount of video traffic in the network from 5 Mbps to 3 Mbps, the absolute number of unsuccessfully protected faults dropped by roughly 95%. When the HTB prioritisation is applied simultaneously, the drop in the absolute number of unsuccessfully protected faults is lower. In addition, it can be observed that the amount of video traffic causing the least unsuccessfully protected faults is 3 Mbps for this particular wireless network.

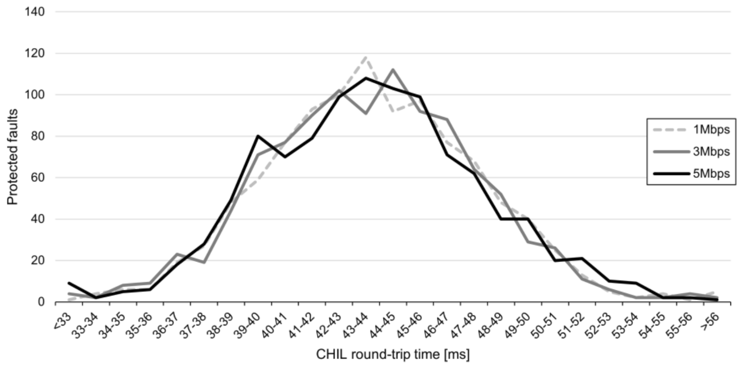


**Figure 18.** Histogram of round-trip times [ms] to protected faults on different levels of video traffic.

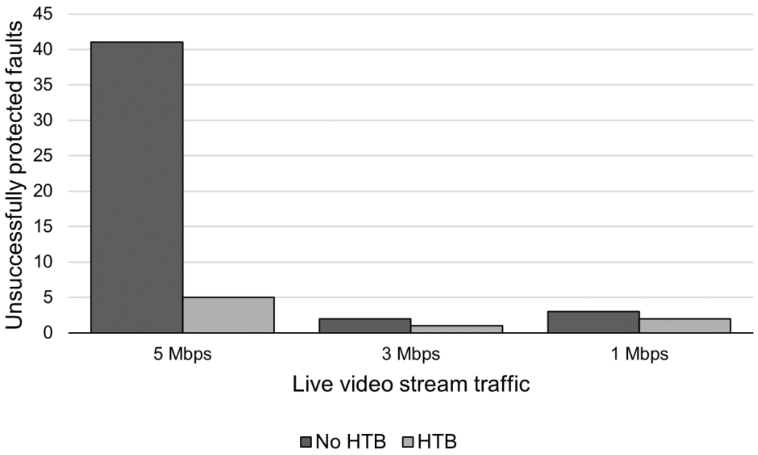


**Figure 19.** An absolute number of unsuccessfully protected faults on different video traffic levels with and without HTB prioritisation from Publication 7.

## 4.3 Discussion on applicability of 5G for protection

Based on the work presented in this thesis, it is clear that 5G SA can be applicable for protection communication, but not without caveats. The suitability of 5G depends largely on each protection application's communication and operational requirements, which can involve several standards, recommendations, and grid operator-specific requirements. Therefore, 5G could be deployed for some applications, such as fault passage indication supported by edge computing, while not yet for others.

The biggest hindrance to the applicability of 5G for protection communication is reliability. Variability of latency and jitter, which naturally occurs in wireless networks compared to wired connections, should be mitigated to improve reliability. Furthermore, other network challenges, such as packet loss, should be equally mitigated by developing the networks and implementing compression techniques for the protection data, as demonstrated in Publication 3. With the existing solutions, the timing of protection operating and network problems occurring is a coincidence, meaning that during a testing phase, the problems in the network might always occur at a different time from the operation of protection. Thus, the protection would always work, while in other cases, the network problems could occur at the same time as the protection communication, thereby incapacitating the protection application. Therefore, it is recommended when assessing the suitability of wireless technologies for protection in a specific case to holistically investigate the operation of the protection system, accounting for selectivity and backup protection.

Furthermore, the geographic location of the protection system overall and each sensor is crucial. Suppose the location does not have reliable and maintained communication networks, and telecommunication providers don't offer wireless connectivity for industrial applications. In that case, there is no sense in implementing protection communication over 5G in such a location. However, grid operators are not limited to public networks. In some cases, operating a private network or purchasing it as a service from a telecommunication provider could be a suitable option. Similarly, great geographic distance between the communicating devices or between the equipment in the field and at the edge could increase the latency beyond the requirements, as shown in the rural scenario of Publication 1.

Apart from geographic location, the cyberphysical location is equally important when protection applications are virtualised and operated on an edge. Cybersecurity is critical when assessing if protection applications could be deployed on edge. As the edge computing offerings and virtualisation of protection applications are still developing, each implementation needs to be assessed case by case to meet the technical requirements and offer a profitable business proposition. If grid operators are expected to bring their clock to the edge, do maintenance on edge, and potentially acquire additional computing power for security solutions, the business proposition might fall short.

Overall, it is crucial to consider protection holistically as a system encompassing all the protection-related equipment and not only individual applications. As this system is one of the backbones of modern society by ensuring a reliable power supply large parts of the world depend on, protection must consist of various applications with different levels of communication requirements, including devices capable of operating alone with no connectivity. While increased levels of connectivity can provide great benefits as novel protection and predictive maintenance applications, critical infrastructure also requires simple manually operated breakers and IEDs to ensure the lights stay on.

# 5. Conclusions and future work

At its launch, 5G promised extremely low latency and high reliability, which are also the main communication requirements of power system protection. Wireless 5G offers intriguing services and solutions, including edge computing support and network slicing. This thesis explores the applicability of 5G for protection communication, mainly through practical CHIL demonstrations. This main objective is to investigate through subresearch questions on prior bottlenecks 5G removes and limitations of 5G in terms of protection applications. Furthermore, the thesis proposes solutions to address the identified limitations.

Initially, 5G was deployed as NSA with a 4G LTE core to smooth the transition from 4G LTE to 5G and enable 5G rollout before large investments to 5G core. However, with the deployment of 5G SA, the latency and reliability were brought to more suitable levels for the strict communication requirements of protection. The first contribution of this thesis was a demonstration of successful fault indication in a commercial SA network in Publication 2. In the SA network, the fault indication application could be used reliably at its default buffer size, and latency was decreased.

The services enabled by 5G were investigated, including network slicing, which would allow splitting the communication channel into independent parallel paths with separate communication services and optimising the channel. The slices could be organised according to the IEC 61850 communication protocols: MMS, GOOSE, and SV. However, with Publication 7, concerns about the lack of granularity of slicing were highlighted, and prioritisation in a slice was proposed. The second contribution of this thesis is the investigation of network slicing granularity and the prioritisation approaches to improve the transmission of protection communication at the substation relative to other communication traffic types, including live video stream.

Another service supported by 5G that was studied was edge computing, which could enable new virtualised applications of protection systems to be flexibly located at an edge detached from physical sensors. The third contribution of this thesis was an investigation of various aspects that should be considered when assessing the implementation of virtualised protection applications on edge in Publication 1. Moreover, in Publication 1, some aspects were studied through CHIL simulations and computational scenarios to provide a practical understanding of virtual fault passage indication on edge. Cybersecurity concerns of deploying protection applications on edge were highlighted in Publication 1.

Publication 4 showcased the impacts of cyberattacks on power system protection, and Publication 5 presented forensic methods to discover and analyse them.

Limitations of 5G were noted for lack of granularity in slicing, and the optimal packet size seemed larger than SV messages leading to unnecessary packet loss. The fourth contribution of this thesis was an investigation of SV message compression in Publication 3. The methodology proposed to combine several SV packets under the same header since the transmission in the wireless network decreased the packet loss without significantly increasing latency.

While 5G is a promising communication technology for protection, it still requires more development in improving reliability and mitigating occasional high latency peaks. Even if 5G offerings, including network slicing and edge computing, could enable novel, virtualised, protection applications, the protection system should be assessed holistically, including applications and equipment not requiring communication to ensure power system operation during network problems, as highlighted in Publication 6.

Future work of applicability to cellular technologies for protection communication still holds several research challenges. Protection applications using wireless technologies should be studied with all the protection applications in a particular grid subsection to investigate which applications could be virtualised and which remain on physical devices. The impact of selectivity, redundancy, and backup protection on the applicability of wireless technologies for protection communication could be considered. At the same time, a timeline of individual fault events and their correspondence with wireless network problems could be investigated to derive probabilities for unsuccessful protection events due to network problems. Finally, the limitations of 5G could be further investigated in conjunction with proposed 6G features to push for 6G standardisation to include solutions to the limitations of 5G for protection communication.

# References

1. IPCC, *Climate Change 2022: Impacts, Adaptation, and Vulnerability*, D.C.R. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [H.-O. Pörtner, M. Tignor, E.S. Poloczanska, K. Mintenbeck, A. Alegría, M. Craig, S. Langsdorf, S. Löschke, V. Möller, A. Okem, B. Rama (eds.)], Editor. 2022: Cambridge, UK and New York, NY, USA. p. 3056 pp.
2. Ritchie, H., M. Roser, and P. Rosado, *CO2 and Greenhouse Gas Emissions*. Our World in Data, 2020.
3. Suhaimy, N., et al., *Current and Future Communication Solutions for Smart Grids: A Review*. IEEE Access, 2022. **10**: p. 43639-43668.
4. Observatory, E.G. *What is 5G?* 2021; Available from: https://5gobservatory.eu/about/what-is-5g/.
5. 61850, I., *Communication networks and systems for power utility automation*. 2022.
6. IEC, *61850-8-1 Communication networks and systems for power utility automation*, in *Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*. 2011.
7. IEC, *61850-5 Communication networks and systems for power utility automation*, in *Part 5: Communication requirements for functions and device models*. 2013.
8. 61850-90-4:2020, I.T., *Communication networks and systems for power utility automation*, in *Part 90-4: Network engineering guidelines*. 2020.
9. IEC, *61850-90-1 Communication networks and systems for power utility automation*, in *Part 90-1: Use of IEC 61850 for the communication between substations*. 2010.
10. IEC, *61850-7-2 Communication networks and systems for power utility automation*, in *Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*. 2010.
11. 34/35.11, J., *Protection using telecommunications*. 2001, CIGRE. p. 175.
12. Elenia, *Technical instructions for medium-voltage connections*. 2023.
13. IEC, *60834-1: Teleprotection equipment of power systems - Performance and testing*, in *Part 1: Command systems*. 1999.
14. Hovila, P., et al. *Cellular Networks providing Distribution Grid Communications Platform*. in *26th International Conference on Electricity Distribution*. 2021.
15. ETSI. *5G*. 2023; Available from: https://www.etsi.org/technologies/5g?jjj=1683897249368.
16. VIAVI. *5G Network Slicing*. 2023; Available from: https://www.viavisolutions.com/en-us/5g-network-slicing.
17. GSA, *Public-Networks April 2023 Summary Report*. 2023.
18. Yufeng, X., et al. *Virtual smart grid architecture and control framework*. in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 2011.
19. Li, J., et al., *Edge-Cloud Computing Systems for Smart Grid: State-of-the-Art, Architecture and Applications*. Journal of Modern Power Systems and Clean Energy, 2022: p. 1-13.
20. Liao, Y. and J. He. *Optimal Smart Grid Operation and Control Enhancement by Edge Computing*. in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 2020.
21. Chen, S., et al., *Internet of Things Based Smart Grids Supported by Intelligent Edge Computing*. IEEE Access, 2019. **7**: p. 74089-74102.

22. Trajano, A.F.R., et al. *Leveraging Mobile Edge Computing on Smart Grids Using LTE Cellular Networks*. in *2019 IEEE Symposium on Computers and Communications (ISCC)*. 2019.
23. Li, Q., et al. *Communication and Computation Resource Allocation and Offloading for Edge Intelligence Enabled Fault Detection System in Smart Grid*. in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 2020.
24. Badmus, I., et al., *End-to-end network slice architecture and distribution across 5G micro-operator leveraging multi-domain and multi-tenancy.* EURASIP Journal on Wireless Communications and Networking, 2021. **2021**(1): p. 94.
25. Horner, L.J. *Using Global Wireless Standard-based Networks to Modernize the Communication Infrastructure Used by Grid Operators*. in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids*. 2022. Singapore: IEEE.
26. Pandakov, K., et al., *Experimental Validation of a New Impedance-Based Protection for Networks With Distributed Generation Using Co-Simulation Test Platform.* IEEE Transactions on Power Delivery, 2020. **35**(3): p. 1136-1145.
27. Blair, S.M., A.J. Roscoe, and J. Irvine. *Real-time compression of IEC 61869-9 sampled value data*. in *2016 IEEE International Workshop on Applied Measurements for Power Systems (AMPS)*. 2016.
28. Hohn, F. and L. Nordstrom. *Data Models and Protocol Mapping for Reduced Communication Load in Substation Automation with High Sampling Rate Protection Applications*. in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. 2018.
29. Luangsomboon, N. and J. Liebeherr. *HLS: A Packet Scheduler for Hierarchical Fairness*. in *2021 IEEE 29th International Conference on Network Protocols (ICNP)*. 2021.
30. Huang, J., et al., *Priority-Based Traffic Scheduling and Utility Optimization for Cognitive Radio Communication Infrastructure-Based Smart Grid.* IEEE Transactions on Smart Grid, 2013. **4**(1): p. 78-86.
31. Narayan Yadav, R., R. Misra, and S. Bhagat, *Spectrum access in cognitive smart-grid communication system with prioritized traffic.* Ad Hoc Networks, 2017. **65**: p. 38-54.
32. Yu, R., et al., *QoS Differential Scheduling in Cognitive-Radio-Based Smart Grid Networks: An Adaptive Dynamic Programming Approach.* IEEE Transactions on Neural Networks and Learning Systems, 2016. **27**(2): p. 435-443.
33. Hindia, M.H.D.N., et al., *Enabling remote-control for the power sub-stations over LTE-A networks.* Telecommunication Systems, 2019. **70**(1): p. 37-53.
34. Zhu, L., et al. *Priority-Based uRLLC Uplink Resource Scheduling for Smart Grid Neighborhood Area Network*. in *2019 IEEE International Conference on Energy Internet (ICEI)*. 2019.
35. Huihui, H., et al. *Implementation of wide area communication in distributed remote video monitoring system for substations*. in *The 2nd International Workshop on Autonomous Decentralized System, 2002*. 2002.
36. Su, Y. and X. Wang. *Video System Linkage Control with Relay Protection in Digital Substation*. in *2010 Asia-Pacific Power and Energy Engineering Conference*. 2010.
37. Hubert, B. *Linux Advanced Routing & Traffic Control HOWTO*. [cited 2023; Available from: https://lartc.org/howto/.
38. ABB, *SMU615 technical manual*. 2023.
39. ABB, *Smart substation control and protection SSC600, Product guide*. 2022.
40. Hajahmed, M.A., et al., *Cognitive Radio_Based Backup Protection Scheme for Smart Grid Applications.* IEEE Access, 2020. **8**: p. 71866-71879.
41. Zamani, M.A., A. Yazdani, and T.S. Sidhu, *A Communication-Assisted Protection Strategy for Inverter-Based Medium-Voltage Microgrids.* IEEE Transactions on Smart Grid, 2012. **3**(4): p. 2088-2099.
42. Brown, D.R., J.A. Slater, and A.E. Emanuel, *A wireless differential protection system for air-core inductors.* IEEE Transactions on Power Delivery, 2005. **20**(2): p. 579-587.

43. Garau, M., et al., *Evaluation of Smart Grid Communication Technologies with a Co-Simulation Platform*. IEEE Wireless Communications, 2017. **24**(2): p. 42-49.

44. An, W., et al., *An Adaptive Differential Protection and Fast Auto-Closing System for 10 kV Distribution Networks Based on 4G LTE Wireless Communication*. Future Internet, 2020. **12**(1): p. 2.

45. Teng, J.-H., et al., *Systematic Effectiveness Assessment Methodology for Fault Current Indicators Deployed in Distribution Systems*. Energies, 2018. **11**(10).

46. Abdel-Latif, K.M., et al., *Laboratory Investigation of Using Wi-Fi Protocol for Transmission Line Differential Protection*. IEEE Transactions on Power Delivery, 2009. **24**(3): p. 1087-1094.

47. Parikh, P.P., T.S. Sidhu, and A. Shami, *A Comprehensive Investigation of Wireless LAN for IEC 61850–Based Smart Distribution Substation Applications*. IEEE Transactions on Industrial Informatics, 2013. **9**(3): p. 1466-1476.

48. Mekkanen, M. and K. Kauhaniemi, *Wireless Light-Weight IEC 61850 Based Loss of Mains Protection for Smart Grid*. Open Engineering, 2018. **8**(1): p. 182-192.

49. Adrah, C.M., et al. *Communication network modeling for real-time HIL power system protection test bench*. in *2017 IEEE PES PowerAfrica*. 2017.

50. Nguyen, V.G., et al. *On the Use of a Virtualized 5G Core for Time Critical Communication in Smart Grid*. in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. 2020.

51. Kumari, N., et al. *Enabling Process Bus Communication for Digital Substations Using 5G Wireless System*. in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. 2019.

52. Jafary, P., 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, 2022. **15**(11): p. 3915.

53. LuotoLuoto, *Advanced technologies ensure the energy revolution towards smart grids and renewables*. 2021, VTT Technical Research Centre of Finland: YouTube.

54. ABB, *Smart substation control and protection SSC600, technical manual.* 2022.

Aalto-DT 152/2023

ISBN 978-952-64-1441-6 (printed)
ISBN 978-952-64-1442-3 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

**Aalto University**
**School of Electrical Engineering**
**Department of Electrical Engineering and Automation**
**www.aalto.fi**