



TECHNISCHE  
UNIVERSITÄT  
WIEN

## Diplomarbeit

# Solutions for Automation of LV-Substations in a G3-PLC Network

(Mögliche Lösungen für die Trafostationsautomatisierung in einem G3-PLC Netzwerk)

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines

## Diplom-Ingenieurs

unter der Leitung von

Univ. Prof. Dipl. Dr. -Ing. Wolfgang Gawlik

(E370 - Institut für Energiesysteme und Elektrische Antriebe)

Univ. Ass. Dipl. -Ing. Stefan Wilker

(E384 - Institut für Computertechnik)

eingereicht an der Technischen Universität Wien

Fakultät für Elektrotechnik und Informationstechnik

von

Behzad Parvin

Matr.Nr. (01329561)

Wien, im November 2020

---

Behzad Parvin

# Abstract

The existing low-voltage networks have so far been designed in such a way that all energy is supplied unidirectionally to the consumers via the local network station. The basis of this was an assumed maximum load per household, to which a corresponding reserve was added. Due to the distributed generation and growing number of decentralized generation plants, the low voltage network becomes more complex. The Energy-flow direction can also be changed, when for example less consumers ask for energy, but through more solar radiation, more electricity produced by Photovoltaic plants. In this described situation, the importance of increasing energy efficiency through flexible demand response and integration of distributed generation power plants with the help of future supply networks: “Smart Grids” comes to the question. The use of existing power cables in PLC (Power Line Communication) seems to be a natural response to communication technologies for smart grids.

To implement the smart grids and smart metering network in PLC environment, Siemens AG developed a communication protocol called AMIS-CX1 (Automated Metering and Information System- Compatibility/Consistently Extendable Transport Profile). This technology implemented successfully in Austria. The disadvantage for this protocol is that it is not an internationally recognized protocol. To fulfill the implementation of smart metering and smart grids in PLC networks, G3-PLC Alliance published series of standards for communication in physical and MAC (Medium Access Control) layer. Currently smart metering communication is established through internationally recognized DLMS (Device Language Message Specification) protocol in the application layer.

As there are no smart grids solution in a G3-PLC network, the idea of implementing a smart metering solution in parallel to smart grids network with an internationally recognized standard, in the PLC network, brought me to a solution to define and establish a separate communication channel for smart grids data packets. To implement this and to fulfill smart grids purposes, smart grids communication is designed through Modbus TCP/IP (Transmission Control Protocol/Internet Protocol) protocol in the application layer for transferring the data from an assumed measuring point to MV/LV Substation.

The test results show implementation of smart metering and smart grids in a PLC network is possible. But for the proper and reliable communication, in specially the noisy and hostile environment of PLC networks, there are significant barriers in the design of G3-PLC protocol.

# Kurzfassung

Die bestehenden Niederspannungsnetze wurden bisher so konzipiert, dass die gesamte Energie unidirektional über die lokale Netzstation an die Verbraucher geliefert wird. Grundlage hierfür war eine angenommene Höchstlast pro Haushalt, zu der eine entsprechende Reserve hinzugefügt wurde. Aufgrund der dezentralen Erzeugung und der wachsenden Anzahl von dezentralen Erzeugungsanlagen wird das Niederspannungsnetz komplexer. Die Energieflussrichtung kann auch geändert werden, wenn beispielsweise weniger Verbraucher nach Energie fragen, aber durch mehr Sonneneinstrahlung mehr Strom von Fotovoltaikanlagen erzeugt wird. In dieser beschriebenen Situation kommt es auf die Frage an, wie wichtig es ist, die Energieeffizienz durch flexible Demand Response und Integration des Distributed Generation mithilfe zukünftiger Versorgungsnetze „Smart Grids“ zu steigern. Die Verwendung vorhandener Stromnetz in PLC (Power Line Communication) scheint eine natürliche Reaktion auf Kommunikationstechnologien für Smart Grids zu sein.

Um das Smart Grids- und Smart Metering-Netzwerk in einer PLC-Umgebung zu implementieren, hat die Siemens AG Kommunikationsprotokoll AMIS-CX1 (Automated Metering and Information System- Compatibility/Consistently Extendable Transport Profile) entwickelt. Diese Technologie wurde in Österreich erfolgreich implementiert. Der Nachteil dieses Protokolls ist, dass es kein international anerkanntes Protokoll ist. Um die Implementierung von Smart Metering und Smart Grids in PLC-Netzwerken zu erfüllen, hat die G3-PLC Alliance eine Reihe von Standards für die Kommunikation in der Physical- und MAC-(Medium Access Control) -Schicht standardisiert. Derzeit wird die Smart-Metering-Kommunikation über das international anerkannte DLMS-Protokoll (Device Language Message Specification) in der Anwendungsschicht (Application Layer) hergestellt.

Da es in einem G3-PLC-Netzwerk keine Smart-Grids-Lösung gibt, brachte mich die Idee, eine Smart-Metering-Lösung parallel mit Smart-Grids-Lösung mit einem international anerkannten Standard im PLC-Netzwerk zu implementieren. Die Lösung basiert auf Definieren und Einrichten eines separaten Kommunikationskanals für Smart Grids-Datenpakete. Um dies zu implementieren und Smart-Grids-Zwecke zu erfüllen, wird die Smart-Grids-Kommunikation über das Modbus-TCP / IP-Protokoll (Transmission Control Protocol / Internet Protocol) in der Anwendungsschicht (Application Layer) für die Übertragung der Daten von einem angenommenen Messpunkt zur Trafostation entwickelt.

Die Testergebnisse zeigen, dass die Implementierung von Smart Metering und Smart Grids in einem PLC-Netzwerk möglich ist. Für die ordnungsgemäße und zuverlässige Kommunikation, insbesondere in der nicht störfreien Umgebung von PLC-Netzwerken, gibt es jedoch erhebliche Hindernisse beim G3-PLC-Protokoll.

# Contents

|           |   |    |
|-----------|---|----|
| 1         | Introduction  | 1  |
| 2         | AMIS Smart Grid Metering System   | 5  |
| 2.1       | AMIS Smart Meters as Sensors for Smart Grid                                       | 5  |
| 2.2       | AMIS System Description   | 6  |
| 2.3       | AMIS Communication  | 7  |
| 2.4       | AMIS Smart Grid Features  | 8  |
| 2.4.1     | Meter Phase Grouping  | 9  |
| 2.4.2     | Voltage Guard   | 9  |
| 2.4.3     | Power Snap-Shot Analysis: “Eyes to the Grid”                                      | 10 |
| 2.5       | Windowed Frequency Hopping System AMIS CX1-Profile                                | 11 |
| 2.5.1     | Physical Layer  | 12 |
| 2.5.2     | Medium Access Control and Network Layer   | 14 |
| 2.5.2.1   | Routing Method: Simultaneous Forwarding   | 14 |
| 2.5.3     | Further Remarks   | 16 |
| 3         | New Generation for Smart Metering in G3-PLC World                                 | 17 |
| 3.1       | PLC Technology Classification   | 17 |
| 3.2       | ITU G. 9903 G3-PLC Standard   | 18 |
| 3.2.1     | History   | 18 |
| 3.2.2     | System Architecture   | 19 |
| 3.2.3     | Physical Layer  | 20 |
| 3.2.3.1   | Physical Layer Specification  | 21 |
| 3.2.3.1.1 | Frame Control Header  | 22 |
| 3.2.4     | Routing in a G3-PLC Network   | 23 |
| 3.2.4.1   | The Lightweight On-Demand Ad hoc Distance-Vector Routing Protocol<br>LOADng       | 25 |
| 3.2.5     | Adaptation Layer  | 28 |
| 4         | Smart Grid Application for Low Voltage Grid Control with G3-PLC and Modbus TCP/IP | 29 |
| 4.1       | Introduction  | 29 |
| 4.2       | Advantages Using PLC for Smart Grid Operation                                     | 29 |
| 4.3       | Disadvantages of Using PLC for Smart Grid Operation: Noises                       | 30 |

|  |    |
|--|----|
| 4.4 Smart Metering Solution with DLMS in the Application Layer | 31 |
| 4.4.1 Application Protocol DLMS                                | 33 |
| 4.4.2 Integration of G3-Protocol in DLMS Architecture          | 34 |
| 4.5 Smart Grid Solution with Modbus in the Application Layer   | 36 |
| 4.5.1 Modbus TCP/IP  | 37 |
| 4.5.1.1 Modbus Messaging on TCP/IP                             | 38 |
| 4.5.1.2 Modbus Components                                      | 40 |
| 5 Prototype Implementation                                     | 41 |
| 5.1 Test Setup   | 41 |
| 5.2 Application Method   | 46 |
| 5.2.1 Calculation of Reaction Times                            | 47 |
| 5.2.2 Signal Lifespan  | 48 |
| 5.2.3 Effects of Noises in the Overall Performance             | 49 |
| 5.2.4 Effects of Joining Process in the Overall Performance    | 50 |
| 5.2.5 Effects of telegram Length                               | 50 |
| 5.2.6 Applicative Baud Rate                                    | 53 |
| 6 Discussion   | 54 |
| 6.1 Experiences in Real PLC Networks                           | 54 |
| 6.2 Conclusion   | 56 |
| 6.3 Outlook  | 58 |
| Literature   | 59 |
| List of Figures  | 62 |
| List of Tables   | 64 |
| List of Acronyms   | 65 |
| Code of Conduct  | 67 |

# 1

## Introduction

The existing low-voltage networks have so far been designed in such a way that all energy is supplied unidirectionally to the consumers via the local network station. The basis of this was an assumed maximum load per household, to which a corresponding reserve was added. Low-voltage grids are currently not designed for a large number of electricity generators based on renewable energy sources. When dimensioning the power lines, the operators depend on estimates based on load peaks in the individual line sections. In order not to exceed specified voltage limits, large safety margins must be planned.

Due to the Distributed Generation and growing number of decentralized generation plants, the low voltage network becomes more complex. The Energy-flow direction can also be changed, when for example less consumers ask for energy, but through more solar radiation, more electricity produced by Photovoltaic plants.

The energy supply of the future faces major challenges, including the steadily growing world population, the pursuit of higher living standards, the goal of reduced environmental pollution and the finite nature of fossil fuels. Without energy, the world's industrialized infrastructure would collapse, including agriculture, transportation, wastewater treatment, information technology, communications and many other basic requirements that are taken for granted in an industrialized nation. An energy shortage that would jeopardize the maintenance of this infrastructure could lead to a population trap.

To supply the people with economical and simultaneously environmentally friendly energy in sufficient quantities is a decisive question of the future.

The electrical energy supply is undergoing a fundamental transformation process:

- For the period up to 2030, annual energy growth of 2.2% is forecasted, and renewable energy sources such as wind power and photovoltaics are expected to increase to 17% [1].
- In addition, the scarcity of fossil energy resources and climate change pose major challenges for the sustainability of energy supply.

All these factors are leading to a paradigm shift in energy networks. For a long time, generation close to consumption and load-controlled operation were considered the basic principles of electrical energy supply. Due to the liberalization and expansion of renewable distributed generation, they are increasingly being questioned.

Since neither wind nor solar energy cannot be stored easily and not in the production unit, the electrical supply systems of the future ("smart grids") will have to be more flexible than they are today. They should continue to ensure a reliable supply, even though they generate energy in a less predictable way. In a sustainable energy system, which is characterized by a high level of environmental awareness, the "consumer" will become a "prosumer", i.e. even

at the lowest network level, the "low-voltage network", decentralized, fluctuating energy generation will increase strongly in the future.

In this described situation, the importance of increasing energy efficiency through flexible demand response and integration of distributed generation power plants with the help of future supply networks: "Smart Grids" comes to the question.

Smart grids technology is still a somewhat undiscovered concept for utilities in many parts around the world. However, it has become central for utilities worldwide to start a process in redirecting their grids to becoming more adaptable in integrating the up-to-date technologies in electronics and ICTs (Information and Communication Technology). A key reason for this is the contribution of a refined energy quality supply on remote monitoring and the regulation of the different electric grid assets. The use of smart metering receives a lot of support from industries and utilities alike due to its potential to create important groundwork for an extensive smart grid. A smart grid that allows for increased savings and commercial possibilities from dynamic connection to the customers' smart meters.

The use of existing power cables in PLC seems to be a natural response to communication technologies for smart grids. For decades, power network operators used AM (Amplitude-modulation) carrier-based communications to move status and alarm messages between power plants and substations and also in operator internal telephony. AM performed on LW (Long-Wave) frequencies, e.g. in the range from 24 kHz to 500 kHz [4]. As a long-haul system, it is able to cap distances of several hundreds of kilometers and has been in prominent use in HV (High-Voltage) lines. The AM bandwidth proved satisfactory for the mentioned applications. These applications can be seen as the first PLC systems.

Bandwidth increased considerably when fiber based optical communications became accessible. Operators had begun to install fiber links in underground cables and overhead using existing poles. Nowadays, because of the high data rate which permits the selling of communications capacity to other operators, it has thus become the standard on HV lines.

Fibers are rarely incorporated in the power cabling of MV (Medium-Voltage) networks. Currently, MV substations connected to the communications network primary through DSL (Digital Subscriber Lines), private pilot cables (copper pairs) or cellular radio techniques.

Since LV (Low-Voltage) lines do not back extra communication cables (e.g. fibers) and like telephony cabling, the 'last mile' in electricity justifies the extensive investment possibilities due to the large number of connected customers. For this reason, PLC becomes an ideal solution to attract many more customers into the smart grid. Furthermore, as customer communication terminals (e.g. electronic meters) positioned mainly underground, radio systems cannot be the best overall solution. Currently the main arguments to implement PLC technology in the LV layer is the smart metering and secondary control of PV (Photovoltaic) power generation and the demand side management.

PLC technology in Smart Grids has been an area of testbed studies and observations in the past decade. In Table 1-1, the requirements of smart grid communication testbed are listed based on results from the summer of 2014 in a regional utility in Germany [4]. The testing condition of artificial background traffic was used to analyze the performance limitations of the communication system. Apart from that the focus was on meter reading with variable readout intervals, fast PV system control and DSM (Demand Side Management).

| Parameter                        | Value                             |
|----------------------------------|-----------------------------------|
| Frequency band used              | 2 to 30 MHz                       |
| Max. PHY data rate               | 200 Mbps                          |
| Max. power consumption slave     | 3 watts (standby)                 |
| Max. power consumption master    | 5 watts (standby)                 |
| IP version                       | IPv6                              |
| Min. no. of slaves addressable   | 1000                              |
| Coupling                         | 3 phase                           |
| Network transparency             | Bridged (transparent to the user) |
| Redundancy for master            | Yes                               |
| Redundancy for slave             | No (optional)                     |
| Addressing                       | Static or dynamic                 |
| Repeater function                | In every modem                    |
| Min. modem distance (comm. span) | 30 m                              |
| Min. data rate (IP layer)        | 10 Mbps                           |
| Max. latency (single hop)        | 15 ms                             |
| Max. unavailability (network)    | 10E-4                             |

*Table 1- 1- PLC network requirements list for a PLC testbed in Germany [4, Page 518]*

To fulfill the implementation of smart metering and smart grids in PLC network, G3-PLC Alliance published series of standards. Key features in the G3-PLC have evolved to meet the hard challenges of powerline communications. This can be seen in G3-PLC's high-speed, highly-reliability and long-range communication throughout the available power line grid. Although earlier developments were overall positive, they were still incapable of addressing the technical requirements needed to sustain the noisy environment of PLC.

These distinct elements present in the G3-PLC allows for the requirements to be met. An example of this is the mesh routing protocol which regulates the best path available between remote network nodes. To improve the communication under noisy channels, the "robust" mode is defined and to choose the optimal modulation mode in neighboring nodes, a channel estimation mechanism is used. In addition, the G3-PLC supports IPv6 (Internet Protocol Version 6) which permits a simple integration of multiple application profiles. This high level of adaptability and flexibility in the G3-PLC creates a promising outlook for its future.

Chapter two discusses the Siemens AG Company solution for smart metering and smart grid with the help of Siemens AG owned developed protocol AMIS-CX1. This protocol is not an internationally recognized communication protocol and during this thesis was studied as a Kick-Off-Motivation to study the possibility of implementation of smart grids. Chapter three goes through the available international standard for implementing smart metering with PLC communication, ITU G.9903. The need for implementing smart metering solution with an internationally recognized standard, brings us to chapter four that introduces internationally recognized solution for smart metering that is currently in use. This solution fulfills the Austrian Energy requirements defined in the document "Smart Metering Use Cases" [6].

As explained, the need for developing smart grid networks left no doubt in the importance of smart grids in our PLC networks. As,

- PLC communication is currently the main and motivating available infrastructure,



- The demand for Smart Metering in Austria and around Europe is currently increasing, and more energy suppliers are seeking for internationally recognized solutions for smart metering,
- ITU G.9903 is the only available international standard that address smart metering and smart grids communication in PLC infrastructure,
- There is currently no available solution for implementing smart grids in parallel with smart metering infrastructure with an internationally recognized PLC communication standard,
- new solutions should consider cost-benefits for companies and is recommended to implemented in current and existing infrastructure,

brought us to the main research question that will be studied in this thesis:

Is it possible to have a smart grid network in parallel with smart metering network without losing the performance?

This led me to propose a method for implementing smart grids parallel with the smart metering network. The proposed method is based on:

- Establishing a separate communication channel in the application layer to transfer data with the help of Modbus TCP/IP Protocol
- A Test-Facility with three one-phase smart meters and a Data Gateway that communicates with Head-End-System (as a simulation for daily routine smart metering data transfer). To simulate possibility of implementing smart grids in the network, with the help of Devolo 500K Modem and Modbus-Simulator (as a simulation for a measuring point), a separate communication channel with Data-Gateway is established.
- This leads us to introduction of the definition of Signal-Lifespan. The main considered criteria for analyzing is:
  - How fast the data packets can be transferred like before (without smart grids simulation),
  - How fast the smart metering average response time can be changed because of smart grids average response time,
  - Regarding response time and data rate speed, what effects can have the emerge of smart grids data packets on the smart metering data packets.
- The test facility is tested in the FCC Band, not in the CENELEC Band (that are all the electric devices for energy suppliers according to EU Regulation should work in this environment). This leads to a more noise-free environment unlike hostile environment of CENELEC Band.

Chapter five presents the test results of the test system with the method proposed in chapter four. A discussion with looking back in experiences in a real G3-PLC network along with conclusion are presented in chapter six.

## 2

# AMIS Smart Grid Metering System

A Smart Grid permits and supports two-way communication between the utility services and the customers using digital technologies and sensing along transmission lines. In this context of a Smart Grid, a smart meter provides a direct connection between End-Customer's electricity needs and the rest of the grid.

In contrast to the traditional electricity meter that just measures the total consumption of electricity in homes, a smart meter can be connected, and thus communicate with in-home displays and devices. This allows us to see how much energy we are using throughout the day dynamically. The type of data can be used to monitor usage during peak and off-peak hours which can consequently help manage overall energy efficiencies and costs. Additionally, the information from the smart meter can be connected to a user-friendly home energy management system which can also be viewed on other external devices like computers or mobile devices.

PLC technology is found to be suitable for home and industry automation usage because of its low 'media cost'. PLC utilizes the existing home and industry infrastructure, thus reducing the need for additional installation expenses, especially new wires installations for high signal penetration. This reinforces a 'plug and play type' use of PLC-enabled systems.

The AMIS smart meters functionality and its communication protocol AMIS CX1 profile of the company Siemens AG is summarized in this chapter. The goal for this chapter is to get to know about one of the available solutions for smart metering and smart grids in PLC network. It looks specifically at AMIS CX1 profile for PLC between electricity meters, breakers and other grid elements and the data concentrator points at central stations in the LV distribution grid. The AMIS CX1 profile is configured as a multi hop master-slave system which describes the layers 1 to 4. In this profile, the data concentrator is always the master and all other nodes are slaves, which respond on demand and when required.

## 2.1- AMIS Smart Meters As Sensors for Smart Grid

Apart from energy consumption measuring, AMIS smart meters collect the value of voltage and help for providing the stability of the energy system. The function "Voltage-Guard" measures the voltage levels in a week, so the areas in the network that have over-voltage or under-voltage can be defined. In these areas with the help of PSSA (Power Snap-Shot Analyze) the reason and cause will be defined. The power snapshot offers the optimal planning method of network extension. In the wake of the need for continuous extension of network, it can be a better solution for estimation of Network load for future use. In this way the network can be used more efficient. Also, photovoltaic roof mounted cells and electric cars provide more network capacity. In other words, More PV Cells and Electric Cars connected to the network without the need for network extension.

AMIS supports the five essential elements in the distribution network [1]:

- Increasing energy efficiency through flexible tariffs and 'Demand Response'.
- Demand response stands for the targeted relief of energy loads on the network grid through the influencing of electricity customer behaviour.
- Increasing operating efficiency through automated metering processes and automated network operation based on an integrated infrastructure concept.
- Integration of decentralised production facilities and
- Ensuring network and supply security.

Smart Grids should ensure the reliability, stability, and sustainability of electricity supply. The basis for this is the use of smart metering and continuous bidirectional communication across all network levels right to the end consumer.

## 2.2- AMIS-System Description

The AMIS system is a holistic solution for recording consumption data and managing distribution networks. It developed from the needs and requirements of the liberalised energy markets and represents a system that is suitable for recording, transmitting, and storing information in a central office. The consumption data accumulated is not only from households and special contract customers but also from the distribution network infrastructure.

AMIS thus provides a foundation for smart grids. Only the automatic and comprehensive recording of consumption data enables network operators to react accurately and dynamically to the increasing challenges of our energy supply.

AMIS gives distribution network operators the opportunity to optimise essential core processes and to offer their customers, both on the supply and the customer side, new services, and data [1]:

- Extensive automation of customer procedures (billing, tariff changes, locking of customer installations, collection processes)
- No restrictions whatsoever with regard to tariff models (several paying models for delivered active energy, time- and / or load-dependent switching) as well as the recording of delivered reactive energy and thus the highest possible flexibility with regard to product design for an energy supplier
- Recording the use of individual line segments and transformers to optimize maintenance intervals, reduce line losses (for example by changing disconnecting points) and obtain extra data for network planning.
- Recording and diagnosing errors and minimising outages.
- Recording and documentation of the customer supply at the end-customer point (meter) for verification purposes and for network planning.
- Support in crisis management in case of catastrophes by a rapid network status survey and activation of simple island network construction in case of limited energy resources (disconnection of customer groups independently and supply power limitation).

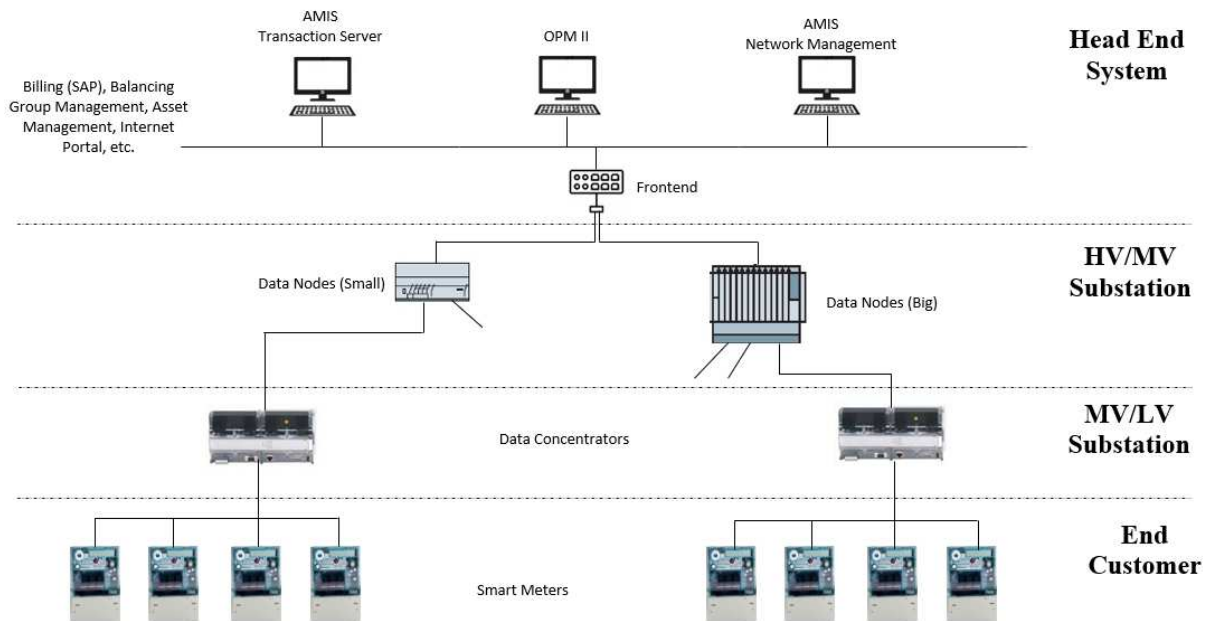


Figure 2- 1- AMIS Configuration Overview

The electronic AMIS multi-functional electricity meters integrate power and energy measurement and the complete DLC (Distribution Line Carrier) communication via the power supply network.

The load-switching device is activated with the use of a timer or by command from the control center.

The data concentrators in the LV transformer stations combine the data from the meters, the load switching devices and the third-party device gateways and can be modularly extended to an automated functionality.

The data concentrators in the substations perform further data concentration and conversion to the required communication interfaces.

The transaction server in the control center makes all the collected and processed data from the terminals available for various applications (billing, load profile data, ripple control, etc.). The automation data from the distribution network infrastructure can be transferred directly to a control system (SCADA).

## 2.3- AMIS Communication

As figure 2-2 showcases, the AMIS solution, as a communication network is based on the first level on the LV network (connection of the end-device with the MV/LV Substation). For this purpose, a narrow-band DLC communication technology was developed based on the Spread-Spectrum Methods. This allows highly available and secure communication via the power grid. The corresponding DLC modems are permanently integrated in the end-devices (meters, load switching devices, third-party device gateways) as well as the data concentrators for the MV/LV substations.

The second level of the communication network (for the connection of the MV/LV Substation with the HV/MV substation) can basically be implemented with any communication medium such as narrow-band radio, IP (Internet Protocol) networks, fiber

optics (FO) and all types of copper cables. The modems or IP components required for this purpose are integrated into the AMIS management system via the data concentrator and can thus be fully remotely monitored and parameterised. As an alternative to classical communication solutions, a special MV DLC method can also be used, which masters the constantly changing of line characteristics and makes network switching invisible to the user via its own routing protocol. In principle, all telephone networks (POTS, ISDN, GSM, GPRS, UMTS, etc.) can also be used for this communication. However, in this case is the limited availability of space, the dependence on third parties, the communication fee and limited investment security to be considered.

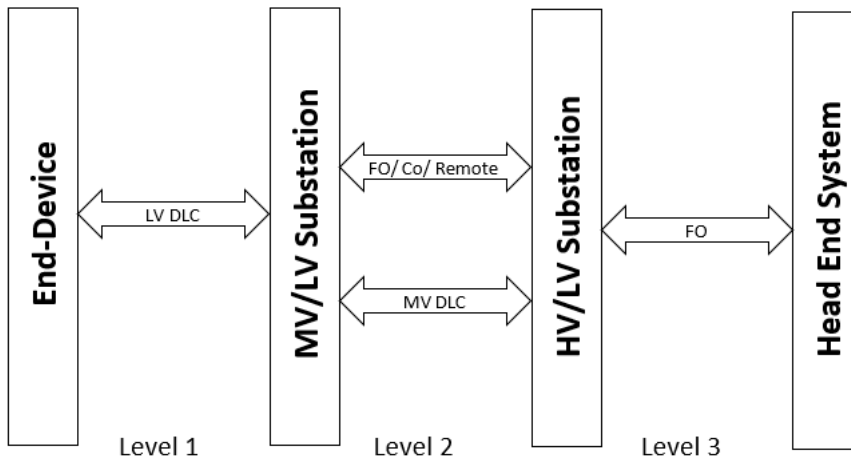


Figure 2- 2- AMIS Communication Model

The third level of the communications network (for connecting the substations with the central office) is usually the existing communications infrastructure of the network operator; however, it can also be freely designed according to the possibilities and requirements, like level 2.

## 2.4- AMIS Smart Grid Features

The actions of smart metering can be compared to a set of eyes reacting and moving according to the grid's operations. The results can help the development of new approaches for network analysis (PSSA & voltage guard) for LV grids. For this reason, the four wire models (three phases plus neutral wire) for LV grids in combination with sufficient simulation data sets should be able to help optimize design of LV grids. The new methods like PSSA will support optimization of utilization (with respect to loads) and the integration of decentralized generation and electric vehicles.

Smart Meters that are in a communication network connected -for every consumer- provide a measuring device for voltage, active power, reactive power. The use of this device provides a new thorough insight in the LV network. The meters so to speak "Eyes to the Grid" and make the future network analysis possible and as a result, optimal use of network capacity.

Following three processes allow an efficient long-time observation and to track the status of every network node.

## 2.4.1- Meter Phase Grouping

The assignment of phases is necessary because in LV networks the phase sequence is identical, but the absolute phase allocation is not known. Meter Phase Grouping enables the exact allocation of the meter's individual phase measured quantities to the correct phase (globally via the local network station).

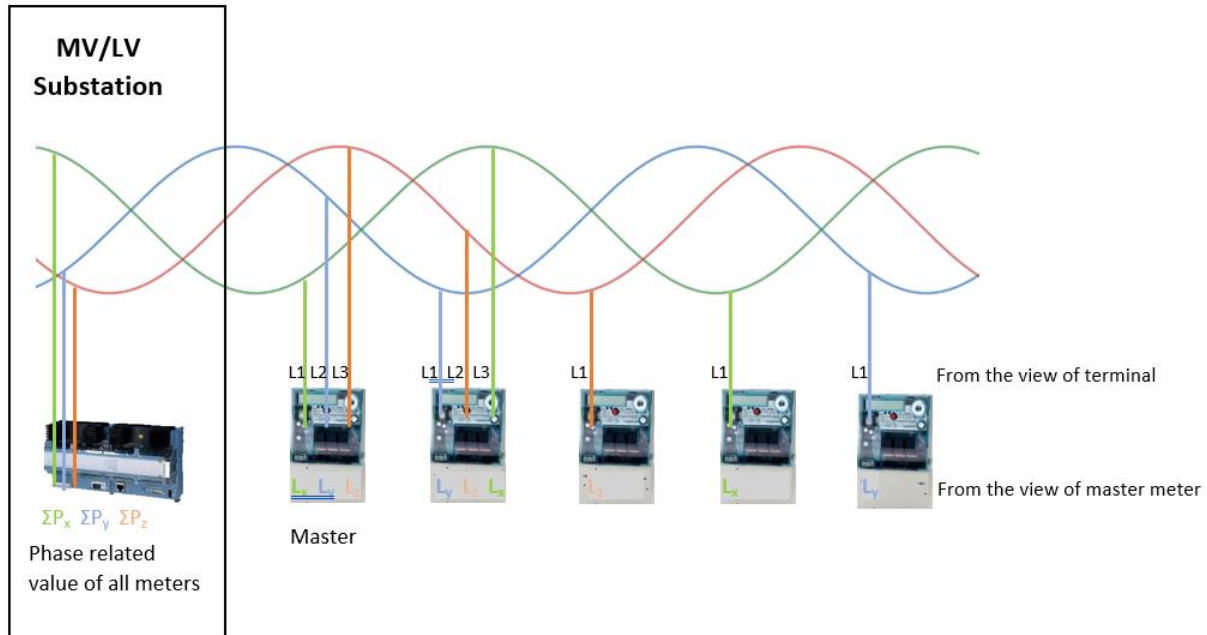


Figure 2- 3- Principle of Phase Grouping

As figure 2-3 showcases, a 3-phase meter is defined as a master meter. In this case, the phase connected to terminal 1 is defined with  $L_x$ . All other meters orient themselves on this.

Starting from the master meter, the offset of the local leftmost phase in each meter is determined. The data of the individual meters are rotated around the offset to the master meter. In this way, the phase values of the individual meters can be added (e.g. power) or compared (e.g. voltage) in the result file. When measuring the total power of a node, the power at the Power Snap-Shot can be compared with the sum of the individual meters (phase-grouped individual power). If the difference between the sum of the individual values compared to the sum measurement is too high (more than the wiring losses), this can be caused by e.g. earth fault currents. If the wiring is unproblematic, the possibility of energy tampering must be considered. High contact resistances at terminal points in the network cause a voltage drop. This causes the voltage to drop in all meters in the terminals. The snapshot can be used to narrow down the location of the meters along the wiring lines if they are arranged locally. The phase grouping is limited between AMIS-DC (Data Concentrator) and the registered end-devices at this AMIS-DC.

## 2.4.2- Voltage Guard:

The collection of time series for every meter goes to an enormous amount of data, that bring a huge attention for data transfer and storage that later for statistic analysis will be needed. So, in the first step the number of meters that are for the observation are needed will be reduced. In these already selected meters instead of time series will be only frequent



distribution collected. The voltage band is subdivided in eleven classes and listed in Table 2-1 [2]. For each 15-minute interval of a calendar week, the average, minimum and maximum 1-second values are classified and counted in the register corresponding to the class. At the end of each calendar week, the histogram data is retrieved and stored centrally. In future, the histogram data of the voltages can be used in the grid design based on the load estimation.

| Class    | Voltage range                |
|----------|------------------------------|
| Class 11 | $U > 111\%U_N$               |
| Class 10 | $111\%U_N \geq U > 109\%U_N$ |
| Class 9  | $109\%U_N \geq U > 107\%U_N$ |
| Class 8  | $107\%U_N \geq U > 105\%U_N$ |
| Class 7  | $105\%U_N \geq U > 103\%U_N$ |
| Class 6  | $103\%U_N \geq U > 97\%U_N$  |
| Class 5  | $97\%U_N \geq U > 95\%U_N$   |
| Class 4  | $95\%U_N \geq U > 93\%U_N$   |
| Class 3  | $93\%U_N \geq U > 91\%U_N$   |
| Class 2  | $91\%U_N \geq U > 89\%U_N$   |
| Class 1  | $89\%U_N \geq U$             |

Table 2- 1- Class distribution of voltage bands

### 2.4.3- Power Snap-Shot Analysis: „Eyes to the grid “

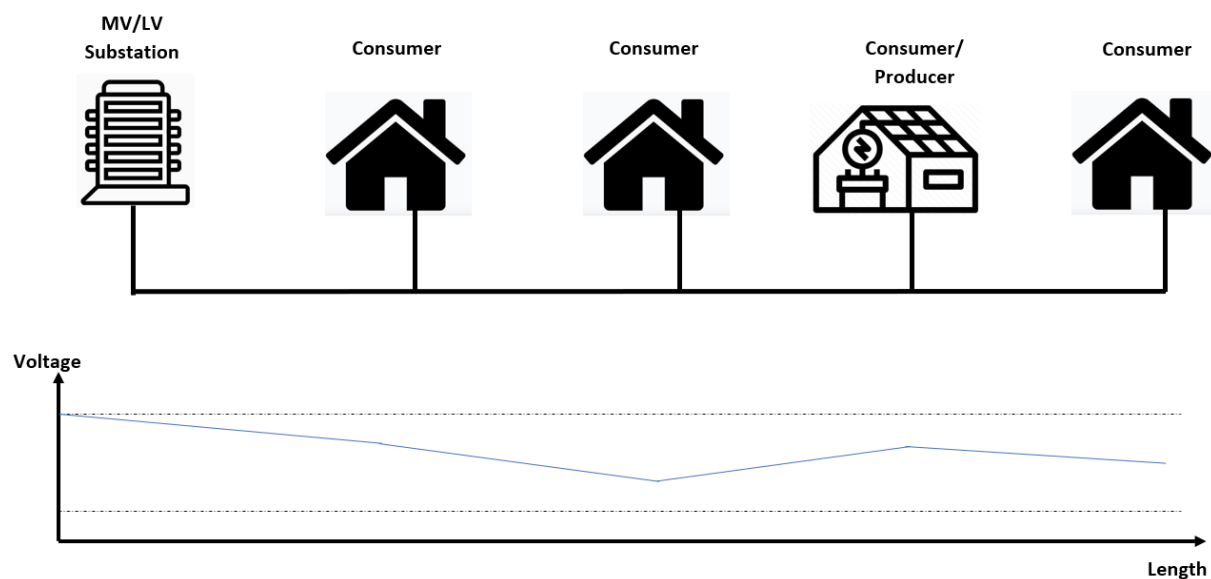


Figure 2- 4- Voltage characteristics along the line in classical LV Network

The voltage characteristics is no longer continuously decreasing over the length of the wiring line but may show local maxima. Inverters raise the voltage so that it can be fed into the grid, so it does not cause over/under voltage. Although inverters only feed in up to a certain upper limit of the voltage, in the case of asymmetrical loads, very pronounced zero-point shifts can occur locally, which can still lead to a dangerous over voltage on individual phases. In such complex grid sections, it is therefore of great importance to know the behaviour of critical parameters to be able to take targeted measures and optimise any necessary investments.

A combination of photovoltaic and an increasing consumption can eventually lead to a line overload: Using Figure 2-4 as an example proves that with the emerge of renewable energies, the insertion of decentralized production (DP) can change the direction of power flow on the distribution network. In this scenario the voltage regulation measurements are playing an important role. Thus, the cable section can be overloaded "unsecured" up to the last consumer.

The AMIS "Power Snap-Shot" (PSS) provides the possibility of recording and providing network-relevant data in a time-synchronised manner, both manually and automatically. In addition, the now real data can be used as a basis for further analysis and thus replaces previously uncertain assumptions and estimated values.

In contrast to the Voltage Guard function shown above, in the Power Snap-Shot, the phase voltages as well as active and reactive powers are only displayed for a moment (1-second effective value) [2]. The technical challenges lie primarily in the required phase allocation and time synchronisation. The measured values are formed synchronously in all meters (maximum deviation 0.1 s) [2]. Phase allocation is necessary because in LV networks the phase sequence is identical, but the absolute phase allocation is not known.

The PSS is a function of the AMIS Smart Grid Metering System for the time-synchronous collection of electrical parameters in the LV grid that are decisive for grid utilisation and for the development of concepts that enable an increasing number of decentralized feed-in systems and optimal utilisation in the LV grids. AMIS electricity meters are used as sensors, which replace conventional meters in the LV network and additionally record relevant network parameters.

The aim of Power Snap Shot Analysis (PSSA) is to create real representations of the stresses in local networks. To obtain the necessary measured values, smart meters must be adapted themselves as measuring devices with corresponding functions in the field. In this way, the potential for implementing the smart grid approach in LV networks is evaluated. Based on this, smart grid models will be developed and evaluated by simulations.

To summarize, PSSA delivers following points:

- Time synchronized measuring of the values
- Delivering all of moment-values
- Analyzing and assignment of the phases
- Analyze and simulation
- Adaption of LV Network model
- Calculation of future scenarios

## 2.5- Windowed Frequency Hopping System AMIS CX1-Profile

AMIS CX1-Profile and its communication protocol uses PLC over the LV distribution grid between final nodes like meters, breakers, control units and data concentrators at central stations. It works as an integrated data management system for utilities and is a classical CENELEC A-Band application according to EN 50065-1. This standard deals with electrical

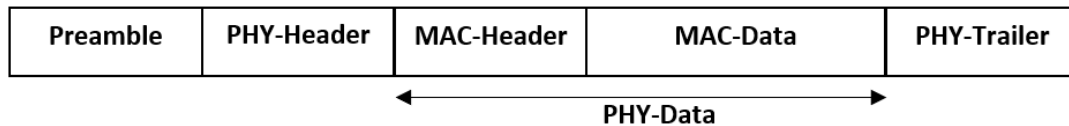


equipment using frequencies in the range of 3 kHz to 148,5 kHz to transmit information on low voltage electrical installations. The frequency bands designated for different applications, output voltage limitations, and conducted and radiated disturbances limitations are specified in EN 50065-1. It was planned for AMIS CX-1 to reach international standardization however it has not yet to become approved. It is neither to be found in the recently approved IEEE 1901.2 (the worldwide standard for narrowband PLC via AC, DC and non-energized electric power lines using frequencies below 500 kHz.) and ITU-T G.990x (introduced in chapter 3) standards.

The layers 1 to 4 (i.e. physical to transport layer) of the OSI model is depicted in the AMIS CX1-profile.

## 2.5.1- Physical Layer

Figure 2-5 shows the packet structure of the physical (PHY) layer. The order of the structure goes as follows: the preamble, trailed by PHY-Header, MAC-Header and MAC-Data, and PHY Trailer. The fixed transmission mode of Preamble and PHY-Header is 600 bits/s[4]. PHY-Data and PHY-Trailer can use one of the 16 transmission modes with data rates somewhere in the range of 600 and 3000 bits/s[4]. The data about the preowned transmission mode is transmitted to the PHY-Header. All transmission modes utilize the frequencies between 39 kHz and 90 kHz and fit into the CENELEC A-Band of EN 50065-1.



*Figure 2- 5- Packet structure of the physical layer of AMIS CX1*

The necessities on the PHY-layer design are marginally distinctive from those for orthogonal frequency-division multiplexing (OFDM) based designs active in IEEE 1901.2 and ITU-T G.990x. Certainly the robustness to frequency selective channels and narrow-band obstructions as well as electromagnetic compatibility is needed.

For these requirements to be met, the AMIS CX1-profile runs with a wavelet-based frequency hopping method jointly with differential phase shift keying (DPSK), interleaving and a repetition code as high redundancy channel coding. By employing a consistent sampling rate of 347.2 kHz (with a deviation of less than 25 ppm), the signal is created. No frequency synchronisation between transmitter and receiver is needed because of the low carrier frequencies. The basic transmission mode consists of a  $(8,1,8)_2$  repetition code, 8 hopping frequencies and a binary DPSK (DBPSK). Other transmission modes utilize  $(5,1,5)_2$ ,  $(6,1,6)_2$ ,  $(7,1,7)_2$  or  $(8,1,8)_2$  repetition codes, 5 to 8 hopping frequencies and either DBPSK or  $\pi/4$ -shifted Quaternary DPSK (DQPSK) modulation. The number of coded bits is continuously equivalent to the number hopping frequencies.

The spreading of the coded bits through time and all the hopping frequencies is guaranteed by a block interleaver. The PHY-Trailer guarantees the blocks are filled for the interleaver

through the process of bit stuffing. A high resistance against narrowband interference and frequency selective fading can be created when every bit of information is transmitted on every hopping frequency. The resistance against impulsive interference is improved because of time spreading. The low code rate of this active repetition code (ranging between 0.125 to 0.2) creates a relatively low data rate. A convolutional code at a code rate of 0.333 to 0.5 would reach an identical or even higher resistance. This could trigger a higher than double data rate with no additional changes to the system.

On the hopping frequencies the wavelets are represented as sine tones with a cosine-roll-off amplitude window with roll-off-factor  $\alpha = 1$ . The big roll-off-factor of  $\alpha = 1$  enhances the spectral forming of the wavelets which is superior to classical frequency hopping approaches. The 50% time-overlapping of these superposed wavelets consequently create a constant and steady envelope. Figure 2-6 clarifies the basic transmission mode in a time-frequency-amplitude diagram. On the Y-axis we can find the hopping frequencies of the basic transmission mode which is activated in a predetermined order with a single wavelet having a duration of  $416 \mu\text{s}$  [4]. The 50% time-overlap results in one wavelet to be transmitted every  $208 \mu\text{s}$ . The  $1.666 \text{ ms}$  of intersymbol-time on individual hopping frequency is constant and after  $1.666 \text{ ms}$  all 8 bouncing frequencies are utilized and it proceeds with the same frequency from the start [4].

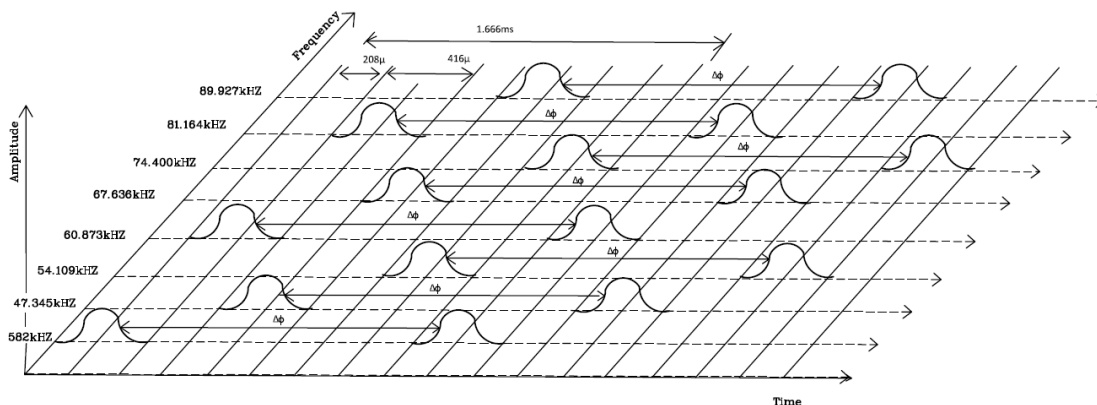


Figure 2- 6- Signals in basic transmission mode of AMIS CX1 (Self depicted based on [4, Page 464])

The phase differences of the consecutive wavelets have mapped the data of the coded bits on the same hopping frequencies. Therefore, the modulation is a temporal DPSK and similar to the differential coding used by the OFDM system in IEEE 1901.2. The OFDM framework would include the successively transmitted signals on the hopping frequencies to a single signal, which would activate all frequencies simultaneously. This results in higher data rates in the OFDM systems. Each hopping frequency is independently used by the modulation scheme of AMIS CX1 and because of the high redundancy and the interleaving method, data is transferred to every hopping frequency individually. Even if only one hopping frequency is transferred reliably, all the information can be delivered.

In comparison to the commonly used OFDM systems for the CENELEC A-band, this approach shows other positive attributes. The available transmit power can be collected on each frequency individually while the constant envelope permits for a more effective transmit amplifier concept. A notch in the access impedance and overload of the power amplifier would only affect a single hopping frequency, as compared to the complete OFDM symbol in other systems. The receiver can do individual matched filtering on each hopping frequency, which has a much better spectral suppression of out of band disturber than an FFT-based

channel (Fast Fourier Transform) separation with a  $\sin(x)/x$  spectral mask. Furthermore, inter-frequency-modulation has almost no negative effect due to non-linearity of the channel. Ultimately, impulsive noise bursts would only hit a single wavelet and not a complete OFDM symbol. Therefore, the AMIS CX1 PHY layer enables PLC over larger distances in the CENELEC A band compared to OFDM-based systems [4].

## 2.5.2- Medium Access Control and Network Layer

The AMIS CX1 communication protocol is configured as a multi-hop master-slave system. In the system the data concentrator acts as the main master and all other nodes are slaves, only acting on demand, sending data when they are called.

AMIS as an unbalanced multi-point communication realized as a serial communication protocol that end-device meters are with a central station with one or more substations through a Line- or Star-Configuration connected. In this communal communication, data transfer is only implemented through the MASTER [5].

All the information from slaves is automatically transmitted to the master via a polling process. All slaves are used as possible repeater and the relay function is realized by synchronous forwarding. This is seen as single frequency network (SFN) based flooding. The inter-connectiveness of synchronous forwarding makes it no longer possible to separate the networking from the MAC. This system design is considered to be a cross-layer approach.

### 2.5.2.1- Routing Method: Simultaneous Forwarding

The system allows up to 8 repetitions of a packet. The transmission mode and the number of repetitions is determined by the master dynamically and individually determined for each slave. Both counters in the MAC-Header gain the added number of repetitions. If a slave receives an undesired packet, and the second counter is not 0, then this packet will be prepared for a retransmission. The second counter gradually decreases in quantity while the CRC for the MAC-Header is re-calculated. Once the packet has been received, exactly 253.8  $\mu$ s after, all the slaves will synchronously re-transmit this prepared packet. This approach can be understood as simultaneous forwarding or as an instance of SFN transmission.

Figure 2-7 showcases a tree topology with 200 participants (cross-markers) using the simultaneous forwarding for a single-packet request-response service. The master can be found the central node. Filled square markers indicate transmissions and square markers receive packets in the indicated time slots. The communication service is activated by the master by sending a request. The message is sent in all directions and is commonly understood as information flooding. Hence, this simultaneous forwarding method can be described as an SFN-based flooding.

In Figure 2-8, we can see how this mechanism is being used by the destination node in the opposite direction. In the example shown, a response arrives at the master via the second repetition which means that a third repetition is not needed. However, by repeating the third repetition, the master gets a second chance to acquire a respond. The needs for

managing the network is independent of the number of repetitions. Regardless of the number of downlinks and uplinks, the number of repetitions will remain constant.

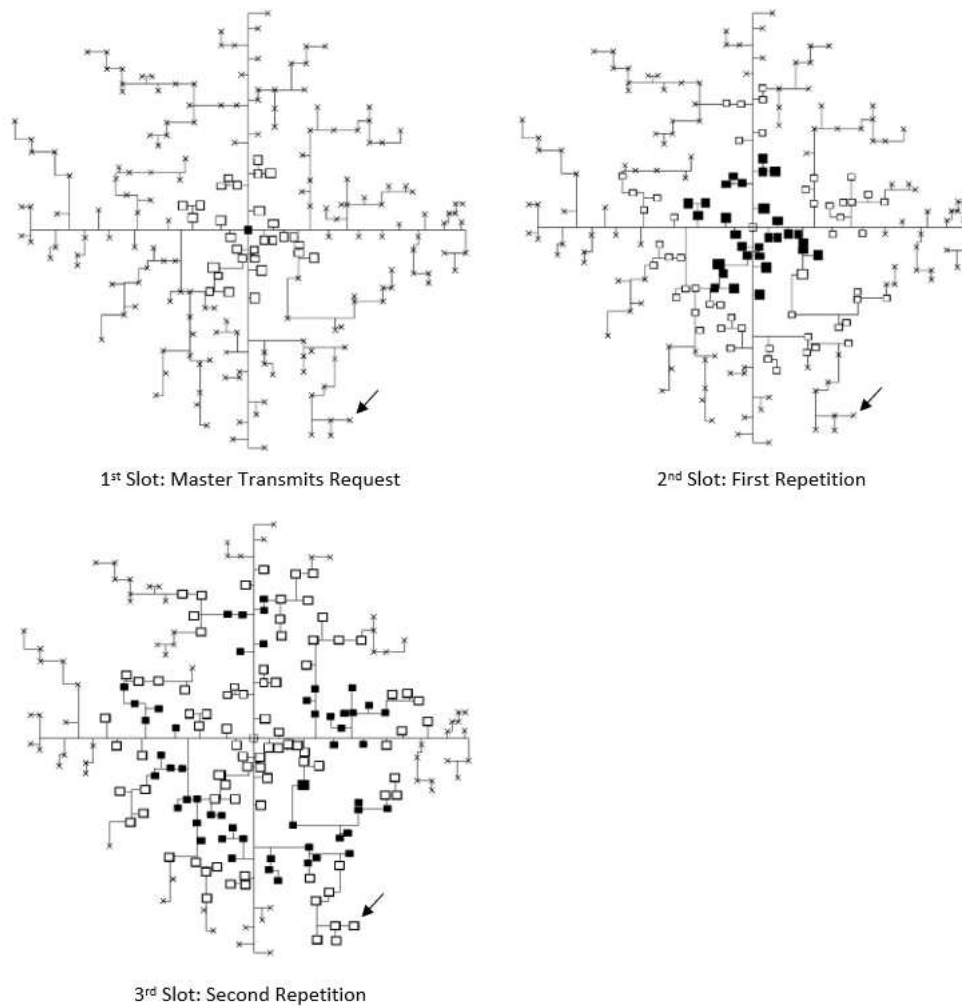


Figure 2- 7- Illustration of Simultaneous Forwarding from Master to destination Slave (--->)  
(Self depicted based on [4, Page 466])

Simultaneous forwarding has a less demanding implementation process compared the routing mechanisms proposed in IEEE 1901.2 and ITU-T G.990x. Due to the fact that repeaters do not need recognition beforehand, the speed of the adaptations to the topological changes can be increased. In any case, due to numerous simultaneous transmissions the in overall energy consumption of the communication system will increase and transmission opportunities are squandered in systems with several repeater levels.

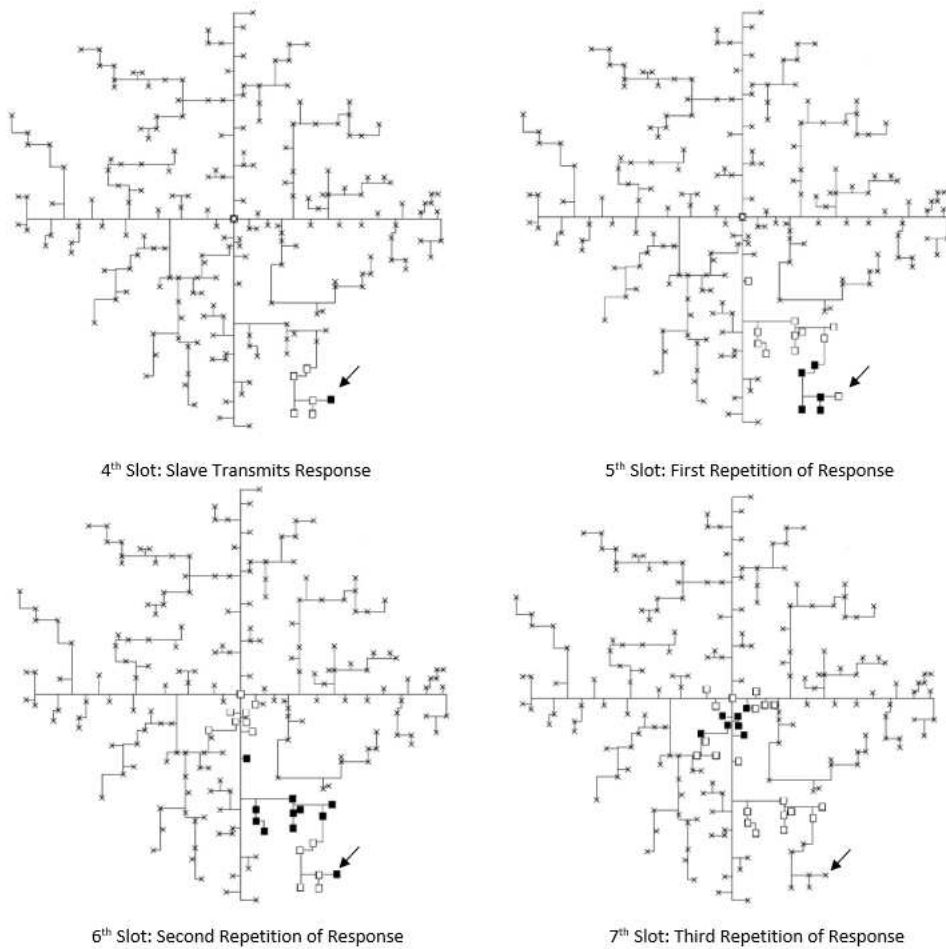


Figure 2- 8- Illustration of Response From Slave to Master in a Simultaneous Forwarding System  
(Self depicted based on [4, Page 467])

### 2-5-3- Further Remarks

The current status of the European Union regulation states that 80% of all households should have smart meters by 2020 [21]. An active case study of the AMIS smart meter system can be found in Energie AG Oberösterreich in Austria [20]. Useful attributes of AMIS CX1 include precise time synchronization, simultaneous forwarding and confirmed broadcasts. Based on the results from this project, AMIS CX1 showcases to be a sound communication solution for smart grid system automation.

# 3

## New Generation for Smart Metering in G3-PLC World

### 3.1- PLC Technology Classification

PLC have successfully shown to be responsive to the next-generation power transmission/distribution systems with end-to-end communication capability, proving that PLC can become a transforming approach in the context of existing power grids. The development of regulation, standardization and certification for PLC, made the field of smart communication with higher data rate and control technologies to be refocused. This progress will positively change the efficiency and security of future power systems, especially in regard to renewable energy resources, distributed intelligence and demand response (DR) programs. As PLC regulations, standards and technologies are being revised and applied to countries from diverse international and national organizations, PLC advancement is in an active developmental phase.

In the sections below, the classification of PLC for smart data communications, focusing specifically on the frequency bands PLC systems which have been in recent use are described. The higher and wider frequency bands used by PLC throughout the decades has made this classification very useful, practical, and popular. The direct impact of frequency bands on signal reach and effective bandwidth will determine the data rate and in turn all the applications possible for future PLC technologies.

PLC systems can be classified as follows [4]:

- Ultra-Narrowband (UNB) PLC: This type of system runs close to 300 Hz to 3 kHz (SLF and ULF bands). An example of this system is the 'Ripple control' system which is mainly designed for one-way communication. They are known to transmit very low data rates (frequently less than 100 bps) ranging over tens to hundreds of kilometers.
- Narrowband (NB) PLC: This type of system works at frequencies between 3 kHz and about 500 kHz. The regulated bands incorporated include; CENELEC A to D-bands defined in EN 50065-1 (Europe, 3–148.5 kHz), the FCC provisions in clause 15.113 of Title 47 of the Code of Federal Regulations (USA, 9–490 kHz), the band specified in ARIB STD-T84 (Japan, 10–450 kHz) and Chinese band (3–500 kHz)[4]. This type of system will often reveal a signal reach and depending on the power grid, can also range over tens to hundreds of kilometers. NB PLC systems have the following subcategories:
  - Low Data Rate (LDR) NB PLC which operate with single carrier modulations for throughputs of hundreds of bps to few kbps.
  - High Data Rate (HDR) NB PLC, which operate with multiple carrier modulations for throughputs up to hundreds of kbps.
- Broadband (BB) PLC: This type of system is often known as Broadband over Power Line (BPL) and it uses frequency bands anywhere from 1.8 MHz to 250 MHz. It can cover



distances from hundreds of meters to a few kilometers, and contains data rates ranging from several Mbps to hundreds of Mbps

## 3.2- ITU G. 9903 G3-PLC Standard

In this section, the recent HDR NB PLC standard developed specifically for smart metering communications is described. The standard can be considered of a second-generation standard because of its long-time use by electric utilities. PLC systems of the first generation have two key characteristics: narrow-band and low data rate (few hundreds of bps to a few kbps) operating at frequencies below 500 kHz. The followings examples are considered first generation PLC systems: ISO/IEC 14908-3 (LonWorks), ISO/IEC 14543-4-5 (KNX), CEA-600.31 (CEBus), X10, Insteon, IEC 61334-5-1/2/4.

Various organizations and institutions in 2010 (particularly industry alliances and standards developing organizations) began a process of standardizing a new generation of PLC systems which would have an operating frequency band below 500 kHz. Multi carrier modulation, especially orthogonal frequency-division multiplexing (OFDM) is used for these HDR NB PLC systems. In late 2012, four separate ITU-T recommendations for NB PLC were approved and published.

In this chapter **ITU-T G.9903 Narrowband OFDM Power Line Communication Transceivers for G3-PLC Networks** is presented. The PHY and the Data Link Layer (DLL) specification for the G3-PLC narrowband OFDM power line communication transceivers is incorporated in this recommendation. It is for operating via alternating current (AC) and direct current (DC) electric power lines over frequencies below 500 kHz.

### 3.2.1- History

In August 2009, the G3-PLC specification became available as an open specification by Maxim Integrated Products, Inc. (USA). It was developed to meet the necessary brief conditions of smart grid applications put out from Electricité Réseau Distribution France (ERDF). The smart grid applications were divided into the following scenarios: grid to utility meter applications, AMI and PEV applications, home automation and home area networking (HAN) communications scenarios. The G3-PLC Alliance, under the leadership of ERDF was formed in 2011. It was established to help support, promote, and maintain this specification. The alliance is made of the following twelve executive members: EDF, ERDF, Enexis, Maxim Integrated Products, STMicroelectronics, Texas Instruments, Cisco, Itron, Landis & Gyr, Nexans, Sagemcom and Triolog [4]. The G3-PLC standard was published in 2012 by the ITU as a recommendation ITU-T G.9903: "Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks".

### 3.2.2- System Architecture

The PHY, MAC and adaptation layers are determined by the G3-PLC standard to help enable IP-based data communication over the low and medium-voltage electrical grids. In Figure 3-1, the communication layers are illustrated which represents the scope of the G3-PLC standard based on the ITU-T G.9903 Recommendation. The main characteristic central to the G3-PLC PHY layer is its capacity for having additional features like adaptive tone mapping, robust mode and two-dimensional interleaving. With these features, the communication through severe noise impairments can have a better performance. G3-PLC is also responsive to LV/MV and MV/LV communication. Furthermore, IEEE 802.15.4-based MAC layer is used above the OFDM based PHY layer. Using the 6LoWPAN adaptation layer, IPv6 packets can be transmitted over the power line channel. The ITU-T G.9903 G3-PLC standard list of parameters are presented in Table 3-1.

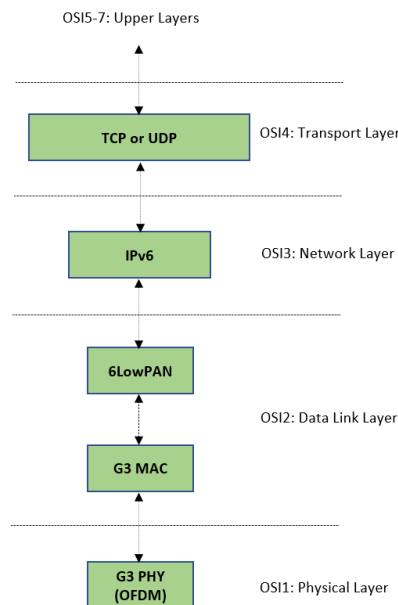


Figure 3- 1- OSI reference model of ITU-T G.9903 G3-PLC standard

|                          |  |
|--------------------------|--|
| <b>Frequency bands</b>   | CENELEC A (35.938 kHz to 90.625 kHz), FCC-1 (154.6875 kHz to 487.5 kHz), FCC-1a (154.687 kHz to 262.5 kHz), FCC-1.b (304.687 kHz to 487.5 kHz) and ARIB (154.7 kHz to 403.1 kHz) |
| <b>Coding/Modulation</b> | OFDM using DBPSK, DQPSK or D8PSK Modulation, optionally BPSK, QPSK, 8-PSK and 16-QAM   |
| <b>Maximum Data Rate</b> | Up to 300 kbps depending on the modulation and the frequency band  |
| <b>Data Link Layer</b>   | IEEE 802.15.4 MAC Frame Format/the adaptation sublayer based on IETF RFC 4944.   |
| <b>Channel Access</b>    | Carrier sense multiple access with collision avoidance (CSMA/CA) mechanism with a random back-off time.  |
| <b>Convergence Layer</b> | IPv6 6LoWPAN   |
| <b>Network Topology</b>  | Mesh Network Routing based on LOADng   |
| <b>Network Formation</b> | Mesh routing protocol  |
| <b>Repeating</b>         | Repeater mode available  |
| <b>Security</b>          | EAP-Pre-shared key, AES-128 key and CCM* encryption  |

Table 3- 1- Major technical features of the ITU-T G.9903 G3-PLC standard [4, Page 522]



### 3.2.3- Physical Layer

Limited bandwidth channels are efficiently used by the OFDM based PHY layer in the G3-PLC standard. The standard can function under the band conditions mentioned in table 3-2:

|                              |                           |
|------------------------------|---------------------------|
| <b>CENELEC A Band</b>        | 35.938 kHz to 90.625 kHz  |
| <b>FCC-1 Band</b>            | 154.6875 kHz to 487.5 kHz |
| <b>optional FCC-1a Band</b>  | 154.687 kHz to 262.5 kHz  |
| <b>optional FCC-1.b Band</b> | 304.687 kHz to 487.5 kHz  |
| <b>ARIB Band</b>             | 154.7 kHz to 403.1 kHz    |

Table 3- 2- Different Frequency Bands Supported by ITU-T G.9903 G3-PLC standard

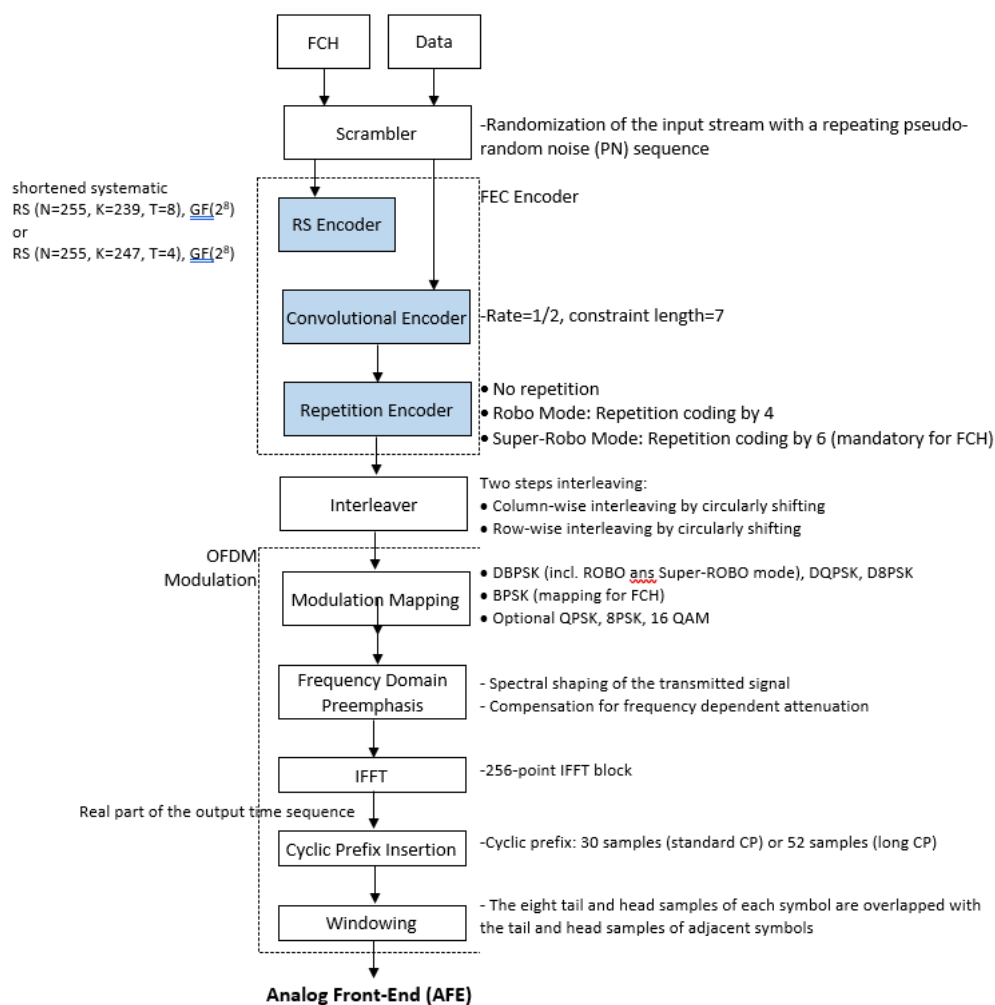


Figure 3- 2- ITU-T G.9903 G3-PLC PHY layer transmitter

The used frequencies will thus determine the maximum number of carriers found in the transmitter is selected to be 128. This will cause a minimum IFFT size of 256 during a CENELEC Band operation, the OFDM sampling frequency is given as 0.4 MHz for CENELEC Band and 1.2 for FCC Band [10]. Therefore, the frequency spacing between OFDM carriers equates to:

$$\frac{400 \text{ kHz}}{256} = 1,5626 \text{ kHz} \quad \text{for CENELEC Band and}$$

$$\frac{1,2 \text{ MHz}}{256} = 4,6875 \text{ kHz} \quad \text{for FCC Band}$$

The tone mask will define the number of carriers and their position in the bandplan which can create various application potentials.

An outline of the PHY layer transmitter process is shown in more detail in Figure 3-2. It demonstrates how the use of Reed-Solomon (RS) and convolutional coding in Forward error correction (FEC) can deliver a better performance against impulsive and burst-type errors. The standard characterizes in normal and robust mode. Data communication is done through two different modes: normal and robust modes. In normal mode, the FEC consists of a Reed-Solomon encoder following with a convolutional encoder. The system also supports Reed-Solomon code with a parity of 8 and 16 bytes. In robust mode the FEC consists of Reed-Solomon and convolutional encoders together with a repetition code. The repetition code repeats each bit four times. According to [10], "Repetition code makes the communication more robust to channel impairments", this of course will reduce the throughput by about a factor of 4".

Regarding OFDM transmitter, "the available bandwidth is divided into a number of sub-channels, which can be viewed as many independent Phase Shift Keying (PSK) modulated subcarriers with different non-interfering (orthogonal) subcarrier frequencies. The OFDM signal is generated by performing inverse fast Fourier transform (IFFT) on the complex-valued signal points produced by differentially encoded phase modulation that are allocated to individual subcarriers. An OFDM symbol is built by appending a cyclic prefix to the beginning of each block generated by IFFT" [10].

To prevent the appearance of burst errors triggered by time and frequency dependent noises, a two-dimensional interleaving scheme are applied. Different modulation constellations like a DBPSK, DQPSK, D8PSK and optional coherent modulation techniques can be supported by G3-PLC. The quality of the received signal will determine the type of modulation scheme the receiver will respond with, to be applied at the transmitter. Thus, each carrier can be modulated up to 4 coded bits per carrier, in similar or different manner. A maximum PHY data rate of up to 300 kbps is supported by the standard [4]. Examples of this are listed in Table 3-3 [4]. The reliability of the whole transmission process can be improved by the switching on and off of the subcarriers with low SNR (Signal to Noise Ratio).

| Frequency Band               | Robo (bps) | DBPSK (bps) | DQPSK (bps) | D8PSK (bps) | Max D8PSK (bps) |
|------------------------------|------------|-------------|-------------|-------------|-----------------|
| CENELEC A (36 kHz to 91 kHz) | 4 500      | 14 640      | 29 285      | 43 928      | 46 044          |
| FCC (150 kHz to 487.5 kHz)   | 21 000     | 62 287      | 124 575     | 186 683     | 234 321         |
| FCC (10 kHz to 487.5 kHz)    | 38 000     | 75 152      | 150 304     | 225 457     | 298 224         |

Table 3- 3- Maximum data rates of ITU-T G.9903 G3-PLC standard at PHY layer

### 3.2.3.1- Physical Layer Specification

The MAC data is modulated by Differential Phase Shift Keying (DPSK), Differential Quadrature Phase Shift Keying (DQPSK) and Differential Binary Phase Shift Keying (DBPSK). A Forward Error Correction is used to ensure that the data is transmitted robustly and as error-free as possible.

As shown in Figure 3-2, a Scrambler, a Reed Solomon Encoder and a Convolutional Code, in cooperation with the Interleaver is used which scatters the individual data bits over frequency and time. In Robust Mode, each bit is transmitted four times. In addition, the data on the MAC layer is encrypted with Advanced Encryption Standard (AES)-128.

Figure 3-3 shows the typical structure of a data frame in the G3 protocol. This consists of a Preamble, which is required for the synchronization of the receiver, and a frame control Header (FCH). The structure of the FCH is defined differently for CENELEC-A-Band and FCC-Band. In case of an Acknowledgement (ACK) at MAC level, no data is transmitted.

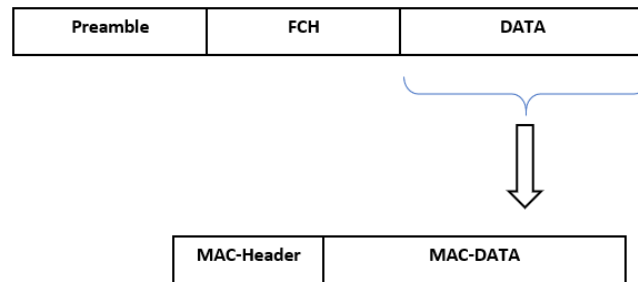


Figure 3- 3- Data Frame Structure of a G3-Frame

### 3.2.3.1.1- Frame Control Header

FCH is located after Preamble and is 5 Byte long. Its main task is to define the telegram type (Delimiter Type(DT)) and with which kind of modulation is the data sent. Also FCH defines phase recognition with the help of a counter (Phase Detection Counter (PDC)). So it is possible to define with which phase the communication with end-device is established.

Figure 3-4 showcases the four different defined DT in ITU-T G.9903 Standard for CENELEC band that can be categorized in two different telegram types [10]. Table 3-4 defines different parameters for FCH [10]:

- Telegrams with DATA : DT=0 and DT=1
- Telegrams without DATA (Acknowledgement): DT=2 and DT=3

ACK-Telegram does not have any Data Field. In this way an explicit allocation of ACK should implemented, because there is not any extra address available (normally it is available in Data Field), the checksum of MAC-Data to acknowledged Telegrams (MAC FCS) in FCH should be filled out. FCH is calculated using a frame control check sequence:

$$G(x) = x^8 + x^2 + x + 1$$

The initial value is 0xFF

The number of subsequent symbols that need to be transmitted are entered in the FCH. Depending on the transmission method (Robust, DBPSK, DQPSK, Differential 8 Phase Shift Keying (D8PSK)), the number of symbols determine the transmitted number of bytes of PHY Service Data Unit (PSDU). This corresponds to the data length of the data field. If data is present, there must also be a MAC header, resulting in the smallest PSDU length of 13 bytes.

|                            | Byte0                |      |      |      |      |      |      | Byte1                                   |      |      |      |      |      |      | Byte2 |      |               |      |      |                |      | Byte3 |      |      |            |            |      |      | Byte4 |        |        |      |     |   |   |   |   |   |   |   |   |   |   |      |      |  |      |  |
|----------------------------|----------------------|------|------|------|------|------|------|---|------|------|------|------|------|------|-------|------|---------------|------|------|----------------|------|-------|------|------|------------|------------|------|------|-------|--------|--------|------|-----|---|---|---|---|---|---|---|---|---|---|------|------|--|------|--|
|                            | Bit0                 | Bit1 | Bit2 | Bit3 | Bit4 | Bit5 | Bit6 | Bit7                                    | Bit0 | Bit1 | Bit2 | Bit3 | Bit4 | Bit5 | Bit6  | Bit7 | Bit0          | Bit1 | Bit2 | Bit3           | Bit4 | Bit5  | Bit6 | Bit7 | Bit0       | Bit1       | Bit2 | Bit3 | Bit4  | Bit5   | Bit6   | Bit7 |     |   |   |   |   |   |   |   |   |   |   |      |      |  |      |  |
| DT=0 (ACK is required)     | PDC= Phase detection |      |      |      |      |      |      | FL (PHY Frame Length N <sub>f</sub> /4) |      |      |      |      |      |      | MOD   |      | TM (Tone Map) |      |      |                |      | 0     |      | 0    |            | FCCS (LSB) |      |      |       |        | DT = 0 |      | PAY |   | 0 |   | 0 |   | 0 |   | 0 |   | 0 |      | FCCS |  |      |  |
| DT=1 (ACK is not required) | PDC= Phase detection |      |      |      |      |      |      | FL (PHY Frame Length N <sub>f</sub> /4) |      |      |      |      |      |      | MOD   |      | TM (Tone Map) |      |      |                |      | 0     |      | 0    |            | FCCS (LSB) |      |      |       |        | DT = 1 |      | PAY |   | 0 |   | 0 |   | 0 |   | 0 |   | 0 |      | 0    |  | FCCS |  |
| DT=2 (ACK)                 | MAC FCS [7:0]        |      |      |      |      |      |      | 0                                       |      | 0    |      | 0    |      | 0    |       | 0    |               | SSCA |      | MAC FCS [15:8] |      |       |      |      | FCCS (LSB) |            |      |      |       | DT = 2 |        | 0    |     | 0 |   | 0 |   | 0 |   | 0 |   | 0 |   | FCCS |      |  |      |  |
| DT=3 (NACK)                | MAC FCS [7:0]        |      |      |      |      |      |      | 0                                       |      | 0    |      | 0    |      | 0    |       | 0    |               | SSCA |      | MAC FCS [15:8] |      |       |      |      | FCCS (LSB) |            |      |      |       | DT = 3 |        | 0    |     | 0 |   | 0 |   | 0 |   | 0 |   | 0 |   | FCCS |      |  |      |  |

Figure 3- 4- FCH Structure

| Parameter                          | Value | Description                 |
|------------------------------------|-------|-----------------------------|
| MOD                                | 0     | Robust Mode                 |
|                                    | 1     | DBPSK Mode                  |
|                                    | 2     | DQPSK Mode                  |
|                                    | 3     | D8PSK Mode                  |
| PAY<br>(Payload Modulation Schema) | 0     | Differential                |
|                                    | 1     | Coherent                    |
| SSCA                               | 0     | No more segment is expected |
|                                    | 1     | More segments are expected  |

Table 3- 4- Parameters for FCH Structure

As shown in Figure 3-3, the data consists of a MAC header and the MAC data. The MAC header is specified according to the IEEE 802.15.4 standard. Figure 3-5 shows the structure of the MAC header in the G3 protocol for CENELEC band with a total length of 12 bytes [22]. The first three bytes are the Segment Control Header, which is necessary for fragmentation. If the Last Segment Flag (LSF) has the value 1, then the last segment was transmitted, or it was a frame without segmentation. The length of the segment would be 10 bit according to the IEEE standard, but since *aMaxFrameSize* in the CENELEC-A band is 252 bytes, the two upper bits are not used (see [10, p. 79]). The segment count is in ascending order starting at 0 and indicates the current segment number in the case of frame fragmentation. The sequence number is incremented with each packet and is identical for all fragments in the case of fragmentation. The MAC header has no source PAN-ID, this is defined by the PAN-ID compression = 1 in the frame control. The length of the source and destination address is defined with 2 bytes (16-bit short address) in the frame control.

MAC-Header Structure

| Byte 0          | Byte 1 | Byte 2 | Byte 3        | Byte 4 | Byte 5       | Byte 6          | Byte 7 | Byte 8              | Byte 9 | Byte 10        | Byte 11 |
|-----------------|--------|--------|---------------|--------|--------------|-----------------|--------|---------------------|--------|----------------|---------|
| Segment Control |        |        | Frame Control |        | Sequence No. | Destination PAN |        | Destination Address |        | Source Address |         |

Segment Control Structure

| Byte 0 |       |       |       |       |       |       |       | Byte 1   |       |                      |       |       |       |       |       | Byte 2 |                                      |       |       |       |       |       |       |  |
|--------|-------|-------|-------|-------|-------|-------|-------|----------|-------|----------------------|-------|-------|-------|-------|-------|--------|--------------------------------------|-------|-------|-------|-------|-------|-------|--|
| Bit 0  | Bit 1 | Bit 2 | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7 | Bit 0    | Bit 1 | Bit 2                | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7 | Bit 0  | Bit 1                                | Bit 2 | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7 |  |
| LSF    | CAP   | CC    | TMR   | 0     | 0     | 0     | 0     | SL [9-8] |       | SC (Segment Control) |       |       |       |       |       |        | SL [0-7] Segment Length of MAC Frame |       |       |       |       |       |       |  |

Frame Control Structure

| Byte 0   |       |       |       |       |       |       | Byte 1   |       |                     |                        |       |       |       |       |       |
|--|-------|-------|-------|-------|-------|-------|--|-------|---------------------|------------------------|-------|-------|-------|-------|-------|
| Bit 0  | Bit 1 | Bit 2 | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7  | Bit 0 | Bit 1               | Bit 2                  | Bit 3 | Bit 4 | Bit 5 | Bit 6 | Bit 7 |
| <b>Frame Type Value:</b><br>0b000= Beacon<br>0b001= Data<br>0b010= ACK<br>0b011= MAC Command |       |       |       |       |       |       | SEC=1  | FP=0  | ACK Requested = 0/1 | PAN ID Compression = 1 | 0     | 0     | 0     | 0     | 0     |
| 0xXX   |       |       |       |       |       |       | 0x88   |       |                     |                        |       |       |       |       |       |
|  |       |       |       |       |       |       | Dest. Add. Mode = 0b10<br>(16 bit short address) |       |                     |                        |       |       |       |       |       |
|  |       |       |       |       |       |       | Frame Version = 0b00                             |       |                     |                        |       |       |       |       |       |
|  |       |       |       |       |       |       | Src. Add. Mode = 0b10<br>(16 bit short address)  |       |                     |                        |       |       |       |       |       |

Figure 3- 5- MAC-Header Structure

### 3.2.4- Routing in a G3-PLC Network

The G3-PLC network topology is built to allow all nodes to communicate with the coordinator and addition, it can incorporate a meshed network structure. The Lightweight On-demand Ad hoc Distance-vector Routing Protocol —Next Generation (LOADng) is administered at layer 2 (L2) as the routing protocol [9 and 10]. This is justified by:

- The necessity to handle looped low voltage grids

- Reaching of multiple routes to the network coordinator,
- The low memory requirements
- Prevention of intellectual property problems.

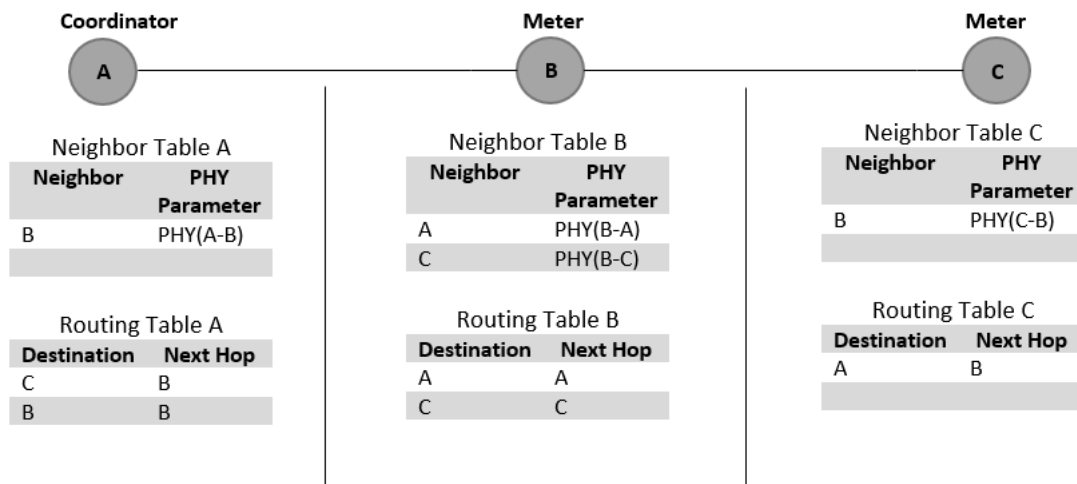


Figure 3- 6- Example of neighbor and routing tables for ITU-T G.9903 G3-PLC MAC layer (self depicted based on [4, Page 524])

For example, in the L2 routing based on LOADng, each MAC packet is allowed to be forwarded hop-by-hop to the destination. Therefore, each network node might be using hopping to transfer a message, hence it can be an indirect or direct transfer. Figure 3-6 outlines how each network node is fitted with a neighbor table and a routing table. The short MAC addresses of the neighbor nodes and the related PHY parameters (like modulation type, tone map, link quality indicator, etc) used for the communication are found in the neighbor table of a node. The direction of the communication determines the PHY parameters since PLC is often asymmetrical. Hence, the quality of the channel will differ based on the communication direction. The G3-PLC standard gives the channel estimation based on tone map request/response which calculates the channel quality. The neighbor table is modified with the reception of either a packet from a neighbor node or a tone map response. The next node to be hopped can be found in the short MAC addresses in the routing table of the node. As a node acquires a MAC packet, the destination node is looked for in its routing table. If the table has the destination stored, the packet will be sent to the next hop in the path. However, if the destination is not present, a route discovery mechanism is activated which helps find the most efficient route to the desired destination. A key element to this is the LOADng protocol which controls the searching and preserving of the bi-directional route to all destinations in the network. If a unidirectional connection is discovered, it automatically gets listed in the Blacklisted Neighbor Set. The list helps prevent similar unidirectional links to be repeatedly selected during this process.

A CSMA/CA mechanism is adopted for channel access in G3-PLC. A CSMA/CA mechanism creates a random back-off time, which is represented as an integer value corresponding to the number of time slots. The main concept parallels to a listen-before-talk approach. The following scenarios help describe the process:

- In the case of a busy channel, the node that wants to transmit a frame waits until the channel becomes idle again.

- In the case that the channel becomes idle again, the node decrements its back-off timer until the busy channel reached again or the timer equals to zero.
- If the channel becomes busy before the timer reaches zero, then the node freezes its timer. When finally the timer equals to zero, the frame will be transmitted by the node.
- A collision happens if two or more nodes decrement their time simultaneously. When this happens, a node has to create a new back-off time.

The application standard will allow access to the channel as a priority. This will activate the urgent delivery of a message.

The G3-PLC MAC layer can give feedback to upper layers as positive and negative acknowledgments (ACK or NACK). It can also execute packet fragmentation and reassembly.

AES symmetric encryption (using a 128-bit shared secret) is found in layer 2 of the network access control and authentication of the G3-PLC standard. AES symmetric encryption is commonly understood as a pre-shared key and these keys are assigned through a coordinator node. Authentication security depends on the available knowledge of the pre-shared key from the other receiving group. Layer 2 provides additional confidentiality and integrity through a cypher counter mode (CCM) type of ciphering. CCM encryption and decryption occurs at every hop in the MAC frames creating confidentiality and integrity.

### 3.2.4.1- The Lightweight On-Demand Ad hoc Distance-Vector Routing Protocol LOADng

In the following section we are looking more thoroughly to the functionality and way-of-doing of LOADng protocol to get to know the routing approach in G3-PLC protocol. It is a reactive MANET (Mobile Ad hoc Network) Protocol which means when a data packet is sent by a router, and the router has no preset route for the destination and thus routes will be discovered.

LOADng is designed to find an optimized route. The criteria is minimum Route Cost (RC) between two nodes in a network. Minimum RC achieved with the help of generating Route Requests (RREQs) by a LOADng Router (Coordinator) as a broadcast message to be received by all LOADng Nodes. RREQ contains:

- RC: the accumulated Link Cost from the originator,
- RREQ ID
- WL: the number of Weak Links
- Originator and Destination Addresses

Upon receiving of an RREQ by the indicated destination:

- A Route Reply (RREP) is created when the address is found in the Destination Address Set or in the Local Interface Set of the LOADng Router [a unicast message, intended to be received only by LOADng Routers on a specific route towards a specific destination originated containing: *RC* which is the accumulated Link Costs from the destination, *RREQ ID*, *WL* and *Originator and Destination Addresses*], in a hop-by-hop approach or unicast manner throughout the installed Reverse Route.



- The RREQ would be used for the future forwarding if the address is not found in the Destination Address Set or in the Local Interface Set of the LOADng Router.
- In the scenario of a broken route (e.g: if a forwarded data packet has been found to fail), a Route Error (RERR) [a unicast message containing: *Error Code* and *Destination Address of the unreachable node*] message rejoins the originator of that data packet which indicates to the originator about the broken route.

Once the optimum route has been found, it is analyzed and passed on to the originator. The communication is triggered by the creation of a unicast RREP message which is then transferred to the originator. For a route to be determined and maintained, the following two tables need to be accommodated by each node:

- **Routing Table** lists the *Destination Address*, *Next Hop Address to the destination*, *Status of a route* and *Lifetime of a route* before expiration.
- **Route Request Table** monitors and oversees the RREQ messages. It processes the RREQ messages during the route discovery. The following information can be found in the table: *RREQ ID*, *Originator Address of a RREQ*, *Forward Route Cost from the originator to the active node*, *Reverse Route Cost from destination to active node* and *Valid Time of the entry* before expiration.

Route discovery only occurs when a source code activates a RREQ message with an incremental RREQ ID and starts to communicate it to its neighbors. Intermediate nodes that accept the RREQ message will add it to its RREQ Table and forward it on. This will only happen if a duplicate RREQ is not found in its RREQ Table. This can be recognized by its RREQ ID and Originator Address. The route to the originator requires it to be consistently added to the node's Routing Table. Additionally, the RC and WL must be kept up to date in the rebroadcasted RREQ. It is important that once RREQs have arrived at their destination and their duplicates are found, that they get disregarded. Duplicates have an identical originator and an identical RREQ ID with a better forward RC (or <RC,WL>tuple) and are discovered in the Route Request Table. If this does not occur, the destination will update the Route Request Table with the newly incoming RREQ. Once it has added it to the table, it will create a unicast RREP and then forward it back through the route to the source node and the RREP is send back to the source code.

Each intermediate node keeps the WL and RC up to date. The control of the RREPs can be achieved because intermediate nodes only forward an RREP when an entry from the exact originator with the exact RREQ ID with worse Reverse RC is found. Then the destination route will be listed in the Routing Table which means the Routing Table is continuously kept up to date with the route to the destination once the originator receives the RREP. A Route Repair can be activated if an intermediate node cannot forward a RREP. This will help find a different route to the source. The final destination then receives a failure report using a unicast RERR message. These nodes which are forwarding the RERRs will delete the originator node from their Routing Table, therefore keeping it up to date.

To compare the Link Cost, based on several parameters such as Modulation (MOD) and Link Quality Indicator (LQI), a mathematical formula is suggested by ITU G. 9903:

$$LinkCost = \max(C_{i \rightarrow j}, C_{j \rightarrow i}) + \frac{AdpKrt * NumberOfActiveRoutes}{MaximumNumberOfActiveRoutes} + adpKh$$

where  $C_{i \rightarrow j}$  and  $C_{j \rightarrow i}$  are the directional link costs (forward and reverse direction, respectively) between  $i$  to  $j$ . The directional link cost is computed as follow:

$$\text{DirectionalLinkCost} = \text{adpKr} * \text{MOD}_{Kr} + \text{adpKm} + \text{MOD}_{Km} + \frac{\text{adpKc} * (\text{MaximumNumberOfTones} - \text{NumberOfActiveTones})}{\text{MaximumNumberOfTones}} + \frac{\text{adpKq} * \text{MaximumLQI} - \text{LQI}}{\text{MaximumLQI}}$$

$\text{MOD}_{Kr} = 1$  for robust mode, 0 for other modulations.

$\text{MOD}_{Km} = 3$  for DBPSK or BPSK modulation (including robust mode), 2 for DQPSK or QPSK modulation, 1 for D8PSK or 8-PSK modulation and 0 for 16-QAM modulation.

$\text{adpKr}$ ,  $\text{adpKm}$ ,  $\text{adpKc}$ ,  $\text{adpKq}$ ,  $\text{adpKh}$  and  $\text{adpKrt}$  as defined in ITU-T G.9903.

Quality measurement of the arriving routing messages create important groundwork for forward direction ( $C_{i \rightarrow j}$ ), modulation, tone map and LQI information. In the case of a reception of a unicast frame, the frame's modulation and tone map configuration can be adopted.

For the reverse direction ( $C_{j \rightarrow i}$ ), the directional link cost may be obtained as in the Figure 3-7. If valid parameters can be found in the neighbor table entry of the destination node, then modulation, tone map and LQI information (for the purpose of computing the directional link cost) will be used from the neighbor table. If this is not the case, the forward link cost will help determine the reverse link cost with this formula:

$$C_{j \rightarrow i} = C_{i \rightarrow j} + \text{adpAddRevLinkCost}$$

$\text{adpAddRevLinkCost}$  represents an additional cost to take into account as defined in ITU-T G.9903

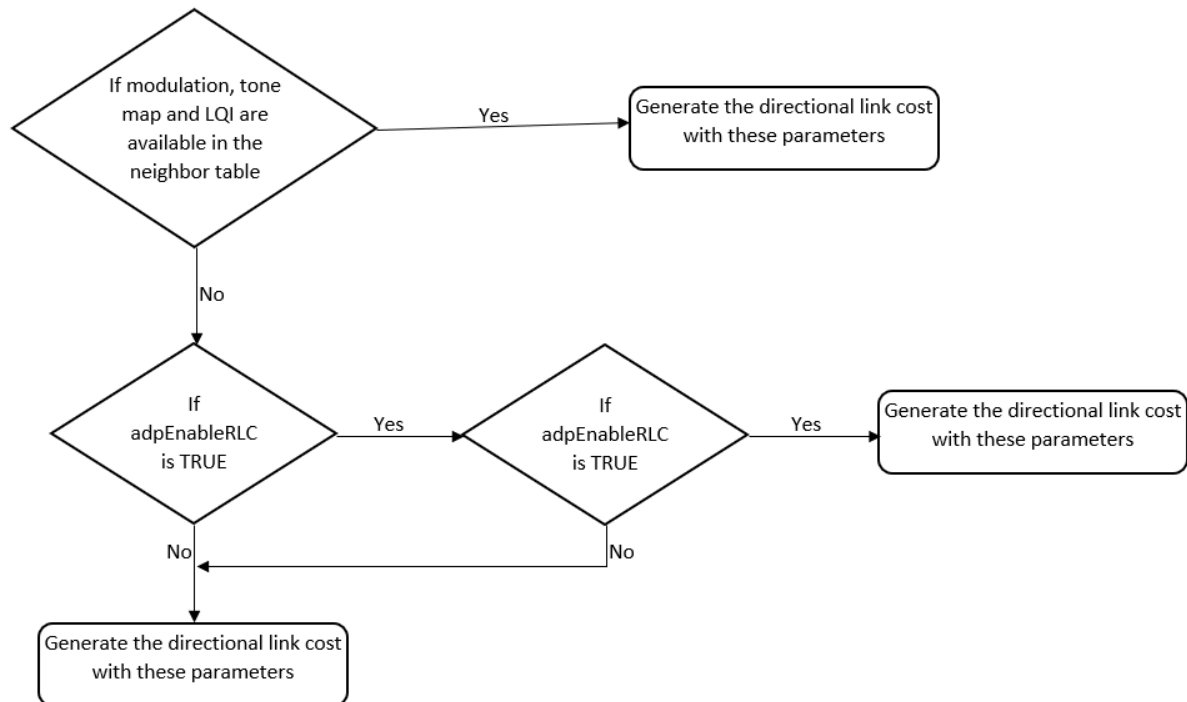


Figure 3- 7- Flowchart explaining the directional link cost computation.  
RLC: Reverse Link Cost



With the discovery of the route, the source and destination will bring that route to the Routing Table. This reinforces the importance of a directional and high-quality route through an asymmetrical channel. This would help prevent frequent route discoveries.

In the case where an intermediate node locates an identical RREQ ID from an identical originator in its Route Request Table, an RREQ is not broadcasted in the LOAD algorithm. This suggests that the first RREQ coming in at any intermediate node has achieved the most efficient and cost-effective route from the originator to that particular intermediate node, as opposed to the later incoming RREQs. However, it must be considered that a better route and route request could have encountered delays at nodes because of processing loads. This issue is dealt with through the rebroadcasting of late RREQs but only in the case when an associated route cost is respectively lower than the previously rebroadcasted RREQ.

When the first RREQ is received, in order to make sure that no other RREQs (ones with a better route cost) are on the way, a predefined period is waited. After this spacing time, the best route is chosen and associated RREP is generated and sent [13].

### 3.2.5- Adaptation Layer

The following two processes of integration are found in the G3-PLC standard. The IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is chosen to adjust IPv6, an internet network layer, into the power line communication.

- 6LoWPAN incorporates the following: layer 2 routing, header compression, fragmentation, and security.
- A network protocol usage is implemented which allows for the transportation of protocols such as TCP, UDP and ICMPv6.

# 4

## Smart Grid Application for Low Voltage Grid Control with G3-PLC and Modbus TCP/IP

### 4.1- Introduction

The integration of current infrastructure of smart metering into a smart grid system is an astonishing step. Smart grid integration with smart metering increases the capability for control applications in other voltage levels of the grid. To achieve the full control of the grid, all LV grid assets need to be controlled in the same approach as other voltage levels.

The conventional LV grid control is available in a way that the records are not well documented like MV and HV grid components. In this case the operational databases are not static and change from one grid intervention to the other. This results to lack of reliable information and weak performance of LV grid operation and maintenance.

Minimum number of considerations that LV grid management should be based on [4]:

- Need for a dynamic smart meter connectivity. In this case there is no need to manually update the connectivity and location of the meter. As a result, through the consistent connection of smart meters it is possible to balance the load of the transformers.
- Need for identifying and locating of grid outages in real time.
- Need for identifying and narrowing down the tampering attempts.
- Need for remote control of LV grid for increasing the reliability in the last component of grid near to the customer.

### 4.2- Advantages Using PLC for Smart Grid Operation

**Connectivity:** A key advantage of PLC communications is the easy intuitive accessibility in connecting to smart meters. Simply put, the smart meter which is connected to a feeder obtains the signal coming from the transformer. This enables an easy identification of the MV/LV transformer which is connected to the various smart meters (in compare to non-PLC communications, e.g. Radio). This characteristic element has the important benefit of reducing the inaccuracies, since often the LV feeder connectivity in utility drawings is inaccurate or not updated.

Transformer connectivity has the following important advantage, firstly in the case of a transformer failure, the utility can determine which customers will get disconnected and secondly, it can efficiently balance the transformer loads connected via three or single

phase. When this information is unavailable, utility procedures commonly will attempt to connect to single-phase customers randomly to each transformer, feeder or phase which is an inefficient and sub optimal approach.

**Non-technical losses:** are the ones that are not related to technical issues. These are mostly caused because of administrative considerations (unknown connections because of administrative errors) or illegal energy tampering. For example, in case of tampering, a way for detecting tampering is double measurement. If we have two smart meters per point of supply (of course one of them is not accessible by the user), the energy consumption at the transformer side can be compared to individual smart meters.

**Outage Monitoring:** Most of the times as a traditional way, outage control is implemented through customer reporting and on-line complaints, but through smart meters disconnection of part of the grids is known through non-availability of smart meters.

### 4.3- Disadvantage of Using PLC for Smart Grid Operation: Noises

Powers lines began transmitting electric powers in low frequencies of 50-60 Hz. This was initially the case because energy moved from a small number of generator sources to a large number of consumer sinks. The PLC data transmissions strongly degrade due to the PLC channel's specific characteristics at higher frequencies. A known drawback of the characteristics of the PLC channel is its lower performance under noise, attenuation and multi-path propagation. This suggests that the interference scenarios undergone in these PLC systems carry some importance. Unlike many other communication systems, "power lines do not represent additive white Gaussian noise (AWGN) channels" [16].

There are five different types of noises which are illustrated in Figure 4-1, that appear in power lines [16]. After transmission of the signal through the impulse response  $h(t)$  of the designated channel, prior to the arrival of the signal to the receiver, these different types of noise  $n(t)$  will be added. According to [16] figure 4-1 illustrates the five types of noises: "colored background noise, narrowband noise, periodic impulsive noise asynchronous to the mains, periodic impulsive noise synchronous to the mains, and asynchronous impulsive noise" [16]. A characteristic of the noise types 1,2 and 3 is their ability to stay stationary over time periods, ranging from possible seconds to hours. Thus, types 1, 2 and 3 belong to the same noise class defined as generalized background noise. On the other hand, types 4 and 5 function on a different time span of milliseconds and microseconds, belonging to the noise class called impulsive noise. Impulsive noise can be further categorized into single pulses and bursts, being able to be specifically determined through experimental measurements [16].

PLC practical experiments have shown that the power spectral density (PSD) of impulsive noises can surpass the PSD of the background noise between a range of 10 dB to 50 dB [16]. This not only suggests that the main cause of error in digital communication over broadband (1.8-250 MHz) PLC networks is impulsive noise but that even when the signal to noise ratio (SNR) is at a relatively decent level, it can still cause errors. Noises at lower frequencies are more energetic which in turn can reduce performance in conventional narrowband PLC

systems. As pointed out in 3.2.3, the functionality of OFDM based PHY layer in impulsive noise environments indicates how it can perform better. The implementation of this modulation method aims at reaching higher data rates, such as a rate of 44 kbps in the CENELEC-A bandplan and a rate of 180 kbps in the FCC bandplan [18].

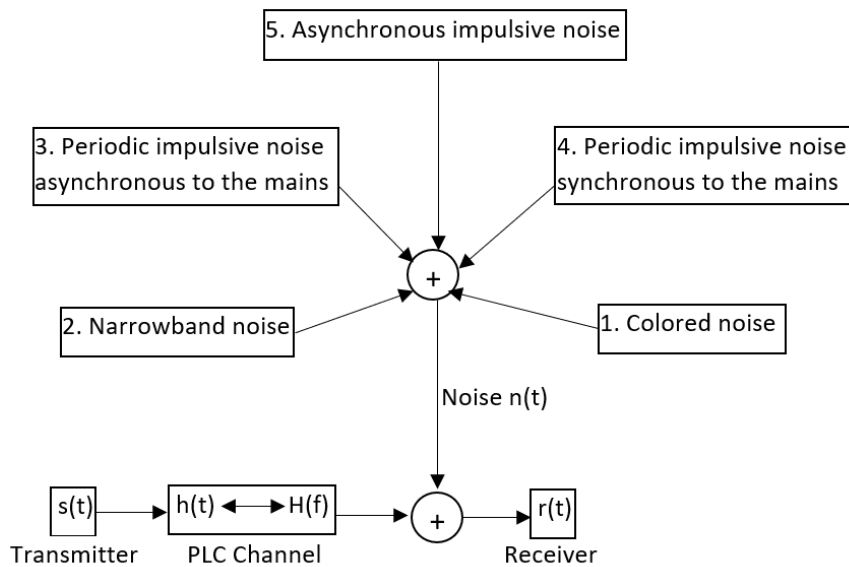


Figure 4- 1- Noise Scenario on Power Line

## 4.4- Smart Metering Solution with DLMS in the Application Layer

The Austrians energy operators have defined a technical solution with the document "Smart Metering Use-Cases". The system architecture also describes the use cases for relevant processes so that uniform test cases can be carried out between suppliers and manufacturers as well as the PSCs (Power Supply Company). The applicable legal framework conditions were taken into account (see [6]).

A reference architecture was described with the OE Smart Metering use cases. Figure 4-2 shows the Advanced Metering Communication System (AMCS) scope, which is defined between Head End System (HES) and Smart Meter (or Electricity Meter). A distinction is made between Last Mile (PLC communication protocols) and Second Mile (LTE, WAN networks). The application protocol that reads the data is transparent and is controlled by the HES. The gateway serves as a communication hub, but no data is stored or decrypted in the gateway.

The OE use case defines a uniform communication connection for the Last Mile, which serves to connect an end device (breaker, smart meter to a gateway), for example an IPV4 or IPV6. Especially for large orders, such as the smart meter rollout for the Vienna networks [25], an interoperable overall system was of central importance to guarantee that there is no

dependence on a meter supplier. The system architecture for this solution of smart metering (Figure 4-3) is shown as an example. Since, according to OE, only a data gateway and not a data concentrator (unlike the AMIS solution described in chapter 2) may be used, the gateway acts as a level and protocol converter. The DLMS protocol is used as an application protocol for smart meters. The HES sends DLMS packets via the gateway to the end-device, which are selectively encrypted for each end-device by the Key Management System (KMS).

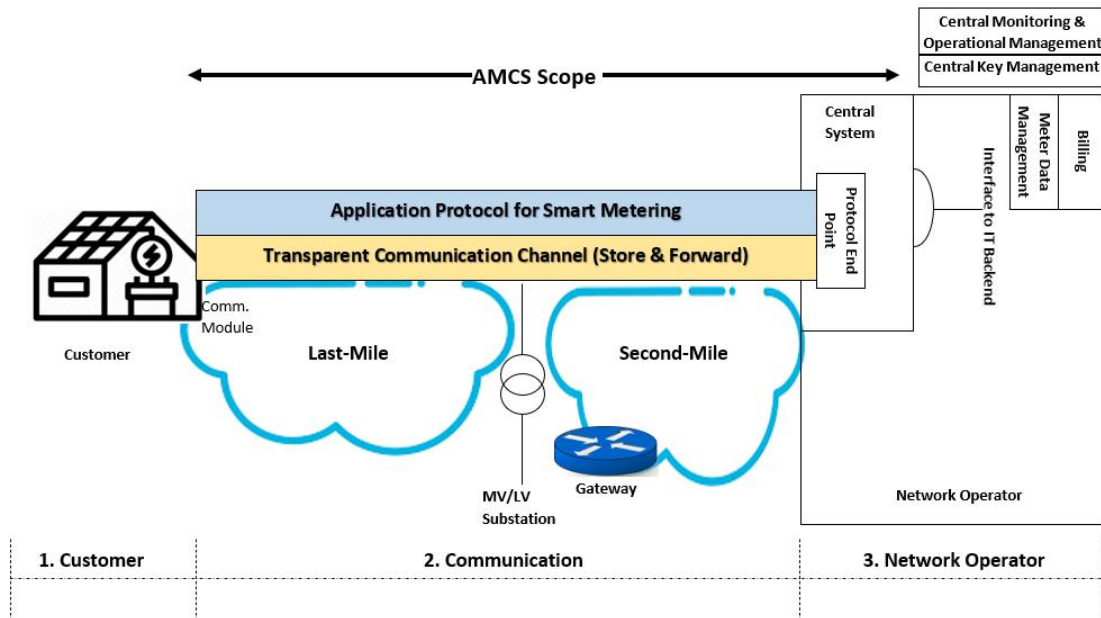


Figure 4- 2- Infrastructure Symbol (self-depicted based on [6])

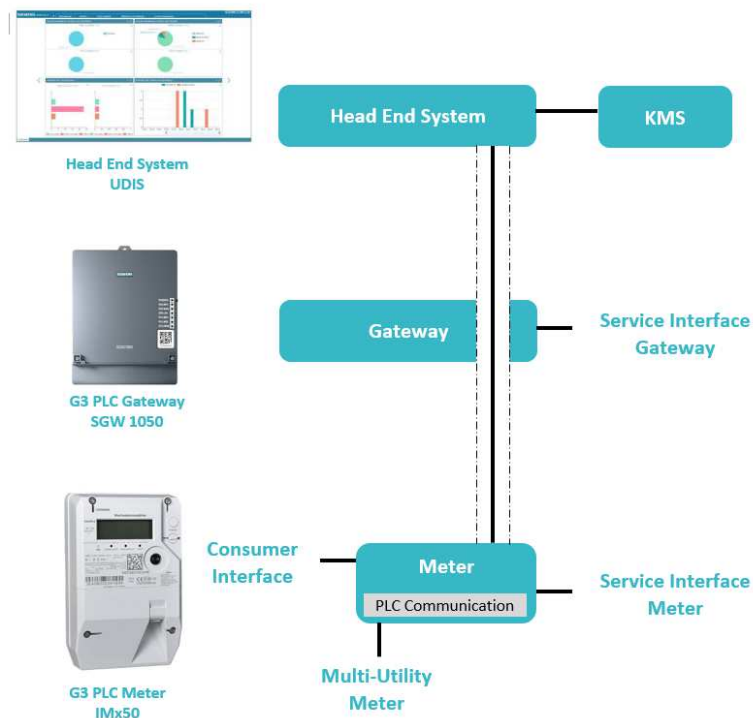


Figure 4- 3- System Architecture of G3-Solution for Smart Metering

## 4.4.1- Application Protocol DLMS

To guarantee interoperability between the individual manufacturers, the DLMS protocol was used as the application protocol. DLMS is an open standard which is written down in the IEC 61334-4-41 standard [23]. This application protocol is not limited to electricity meters but can also be used for other meters (gas, water and heat). The data DLMS Application Protocol Data Unit (APDU) is generated by the DLMS Client in the HES and then encrypted in the KMS.

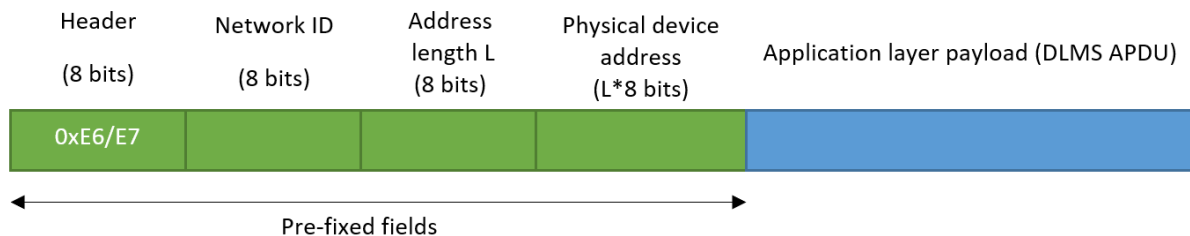


Figure 4- 4- Gateway Protocol Header

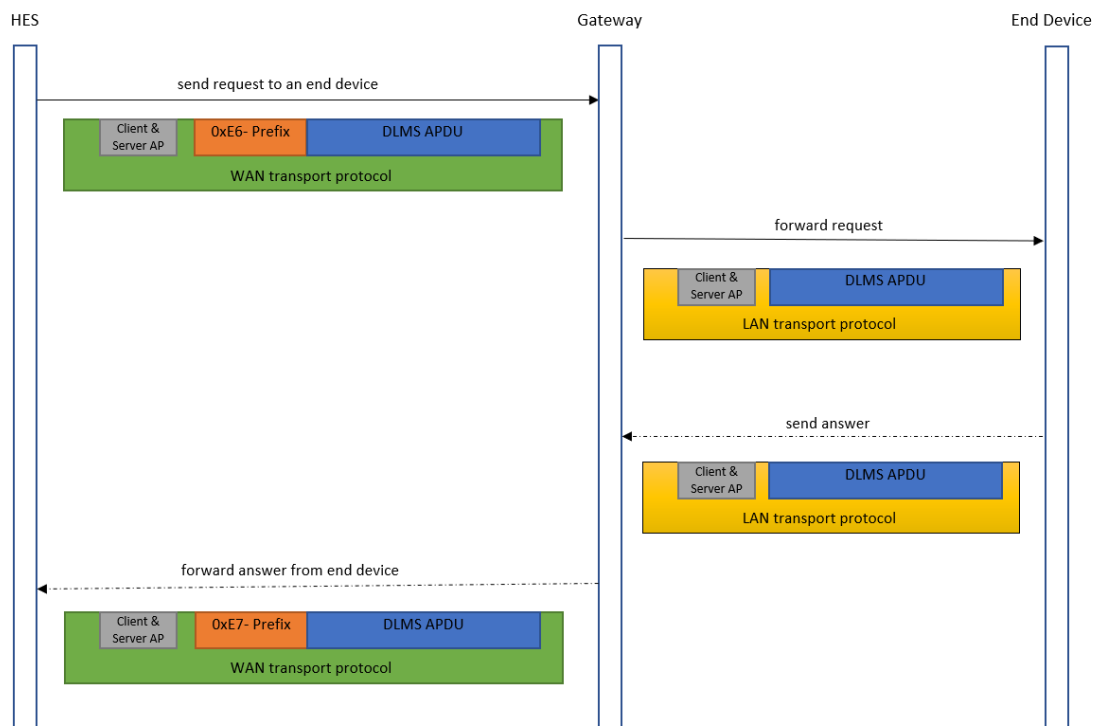


Figure 4- 5- DLMS request from HES to End-Device with Gateway Protocol

Figure 4-4 showcases the structure of the additional Gateway Protocol Header according to DLMS Green Book. The first byte defines whether it is a Request Message (0xE6) or Respond Message (0xE7). The second byte is a network ID and can be freely defined depending on the application (normally the value 0x00 is entered). The third byte specifies the address length. Since the address is an Extended Unique Identifier (EUI)-64 address, this length is always eight bytes. The EUI-64 is the MAC address of the end-device.

Figure 4-5 represents a Pull Sequence from an HES to an end-device. In this configuration, for the Wide Area Network (WAN), Transport Protocol TCP with IPv4 and for the Local Area Network (LAN), Transport Protocol User Datagram Protocol (UDP) with IPv6 is used. In the gateway, the gateway protocol header is evaluated and the application layer payload (DLMS-APDU) is entered in a UDP packet for IPv6. The IPv6 address is determined based on the EUI-64 number of the Gateway Protocol Header.

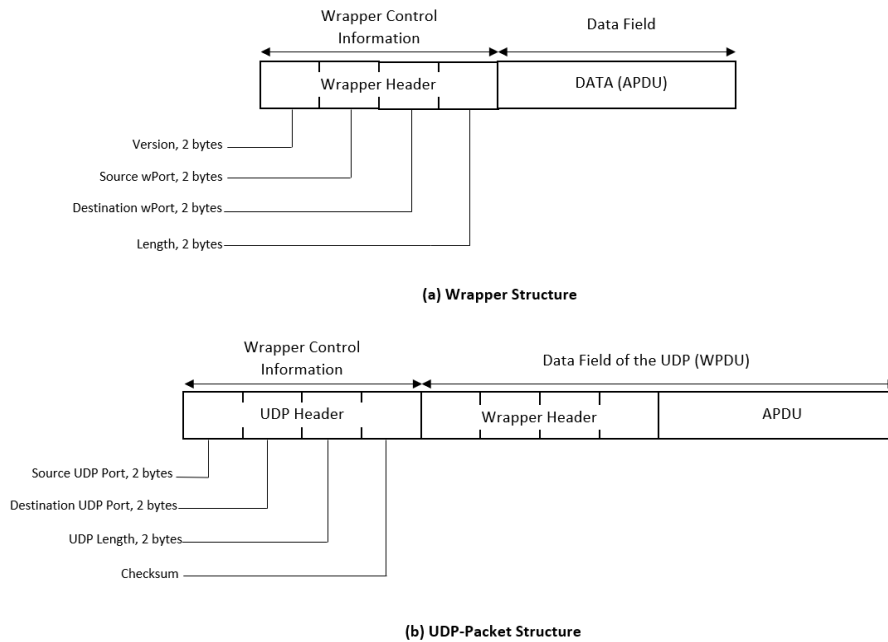


Figure 4- 6- DLMS COSEM UDP

Figure 4-6 shows the structure of a UDP packet for G3-PLC communication. Source and destination wPort of wrapper headers will specify the Port of the DLMS application server. The source port in the send request specifies the role of the user (e.g. Admin, Security, Operational Management). Source and destination UDP port numbers are freely configurable in the end-device and therefore must be parameterized in the gateway. The total Maximum Transmission Unit (MTU) size to be transmitted consists of the UDP header, the wrapper header and the APDU. For the WAN interface the wrapper control information is entered before the Gateway Protocol Header. In the gateway, if the Gateway Protocol Header is removed, the length in the wrapper header must be corrected.

#### 4.4.2- Integration of G3-Protocol in DLMS Architecture

As described in the last chapter, the G3 protocol is thoroughly defined in International Telecommunication Union (ITU)-T G.9903. With the knowledge of G3 System architecture explained in the last chapter, Figure 4-7 shows the integration of this international standard in the DLMS architecture.

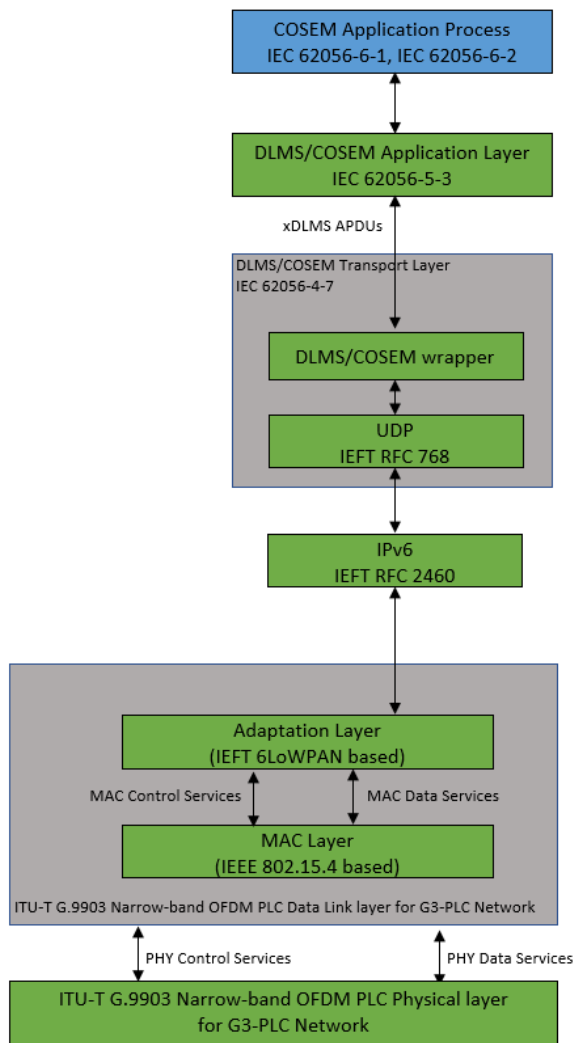


Figure 4- 7- Integration of G3-Protocol in DLMS Architecture

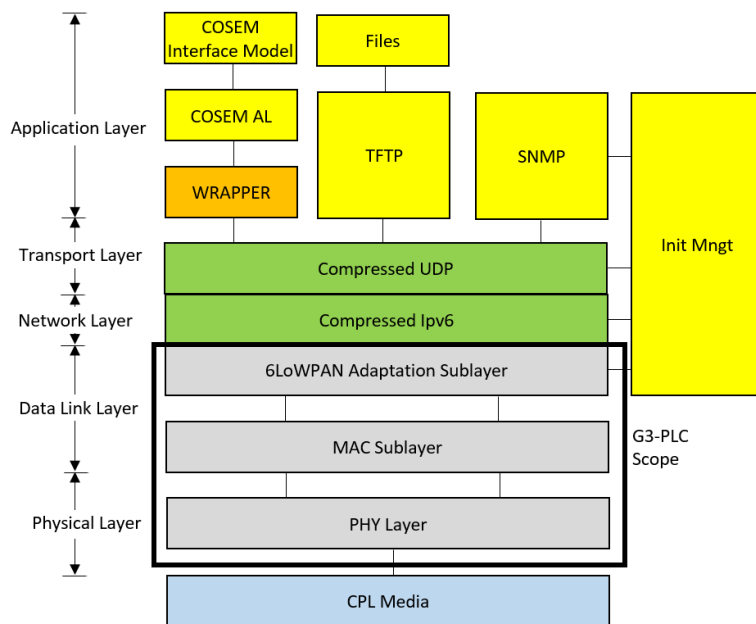


Figure 4- 8- Integration of G3-Protocol in OSI Model (self-depicted based on [7])



The DLMS Application Layer generates a DLMS APDU data frame and adds a DLMS/COSEM wrapper to this package (structure see Fig. 4-5.a). Then this entire frame is entered into a UDP packet and transferred to the IPv6 socket for transmission. The adaptation layer, which is based on Internet Engineering Task Force (IETF) 6LoWPAN, converts this packet and passes this frame to the MAC layer for transmission via a MAC Control Service. The G3 MAC sublayer (Fig. 4-8) is part of the Data Link Layer and is based on the International Standard Institute of Electrical and Electronics Engineers (IEEE) 802.15.4. The 6LoWPAN Adaption Header is also responsible for the fragmentation of the IP packet.

## **4.5- Smart Grid Solution with Modbus in the Application Layer**

As discussed in the chapter two, the AMIS smart meters, apart from its job to collect consumption/produce energy values for smart metering purposes, act as the same time as a measuring device for smart grids purposes and were communicating with two protocols AMIS CX1 and EGDA that both developed by Company Siemens AG. Unlike AMIS Project, the current available smart meters in the market, communicating through international standards like G3-PLC, are only smart meters for smart metering purposes and cannot work as a measuring point for smart grids network.

The main scientific question that in this project will be answered is if it is possible to have a smart grid network in parallel with smart metering network without losing the performance. The goal is to find a way in G3-Network with PLC, to pick up and gain the data and requests fast and efficient, in order to bring network stability analysis.

For implementing smart grids, a wide range of different technologies like Intelligent appliances like smart sensors, smart substations in the LV side or HV side, integrated communications like programmable logic controller, are currently used. These technologies either use wireless communication like cellular, 900 MHz, ... or wired communication like PLC, Fiber, .... What distinguish this thesis from other available smart grids solutions, is the proposed method. This method is based on PLC communication with the help of intelligent smart meters through G3-PLC network. Our analyze is focused on data communication in the LV side in G3-PLC-Interface.

The practice method used in this work is defined through establishing a separate communication channel with Gateway with the help of Modbus TCP/IP. In this configuration, the application Modbus uses Transport Protocol TCP with IPv6 to communicate with gateway.

Modbus is a protocol that is used in the automation technology for LV Network for measuring devices. Modbus is a communication protocol “widely used in process control industries such as manufacturing” [24]. It was created to transfer control data between controllers and sensors using serial and Ethernet (TCP/IP) connections [24].

Modbus is a plain protocol and is used in many measuring devices that are available in the market for messaging purposes. As an example, “PowerLogic ION meters are compatible with Modbus networks as both slaves and masters, and can communicate easily with ION

Enterprise, ION Setup or third-party software” [24]. Also, Siemens AG power monitoring device SENTRON PAC3200 supports Modbus TCP via Ethernet Interface [12]. This wide use of Modbus in measuring devices makes us sure that the proposed method in this thesis can be extended for future developers and manufacturers.

In Modbus a small bandwidth with a shorter header is used, so the most payload can be transferred.

Regarding other possible protocols, theoretically it is possible to use other protocols like DLMS or IEC 61850. But if any protocol is used, it should be considered if other measuring devices in the market can use or support this protocol or not. For example DLMS can be used in smart grids when all smart grids measuring devices also operate in DLMS, or for example IEC 61850 is mostly used in MV automation substations, but for that to be used in LV networks, a larger bandwidth is needed and also if it is really possible to use it in LV network, should be researched and see if there is a market need for LV measuring devices in IEC 61850 in direction of smart grids.

From economical point of view, the choice of appropriate international standard protocol depends on the market needs. Since looking from the view of automation technology manufacturers, development of smart grid devices cost in million euros and cost-benefit-analysis should also be considered. The available measuring devices in the market are supporting Modbus protocol. Considering the market availabilities, for implementing smart grids, establishing a communication channel in LV network that understands Modbus for communication between Gateway and measuring devices is needed.

Regarding security, the question that should be answered is WHERE we want to apply it. The recommended way in G3-PLC protocol [10] is to provide a secure channel in G3 level (Physical layer), then an encryption should be through pre-shared key at LV side implemented. The Data on the MAC layer is encrypted with AES-128 [10]. Based on the experiences, the lasting secured network protocol is not available, because there is always the threat of any kind of protocol hacking. The solution is establishing a secure channel to network. This means, protocols are not always secured, but transfer channel is secured, and the security of the communication protocol (in this case Modbus) not to be hacked is not considered, but in an encrypted G3-level.

Also, another question that around the security issue should be answered is WHAT is intended to protect. For example, in DLMS-level the data (smart meters energy values) are encrypted because of confidentiality of the energy values. Also, for the G3-level the data are encrypted because of authenticity. This means the data for smart grids are pure measuring values and should always be checked if they are valid and are transmitted correctly through transmission path to the central.

#### **4.5.1- Modbus TCP/IP**

Modbus is known as a data communications protocol in the application layer. Modbus was at first published by Modicon (now Schneider Electric) in 1979 in order to be used for programmable logic controllers. The Modbus standard is still able to sustain the

communication of millions of automation devices. In the present day, the admiration of Modbus as a simple but holistic design is still on the rise. Even with the internet community's ability to access Modbus at a reserved system port 502 on the TCP/IP stack encourages its elegant structure even more. Modbus is an application-layer messaging protocol, located at level 7 of the OSI model which supports client/server communication among devices connected on a range of buses or networks. It is also a request/reply protocol where services are determined by different function codes and are distinct elements of Modbus request/reply PDUs (Protocol Data Unit).

The TCP and IP work together and function as the transport protocol for the IP. Information from Modbus use these protocols by receiving the data, then moving it to the TCP where new information is added and then it is passed on to the IP. After that, the information is collected in a packet or a datagram and then transmission starts. Since TCP is a connection-based protocol, it is firstly required for a connection to be built before any transferring can begin. So, firstly the Master (or Client in Modbus TCP) creates a connection with the Slave (or Server) and the Server awaits the connection from the Client. When a connection is found, the Server can respond to the Client, who also decides when the connection closes. Figure 4-9 showcases the construction of a TCP/IP ethernet data packet.

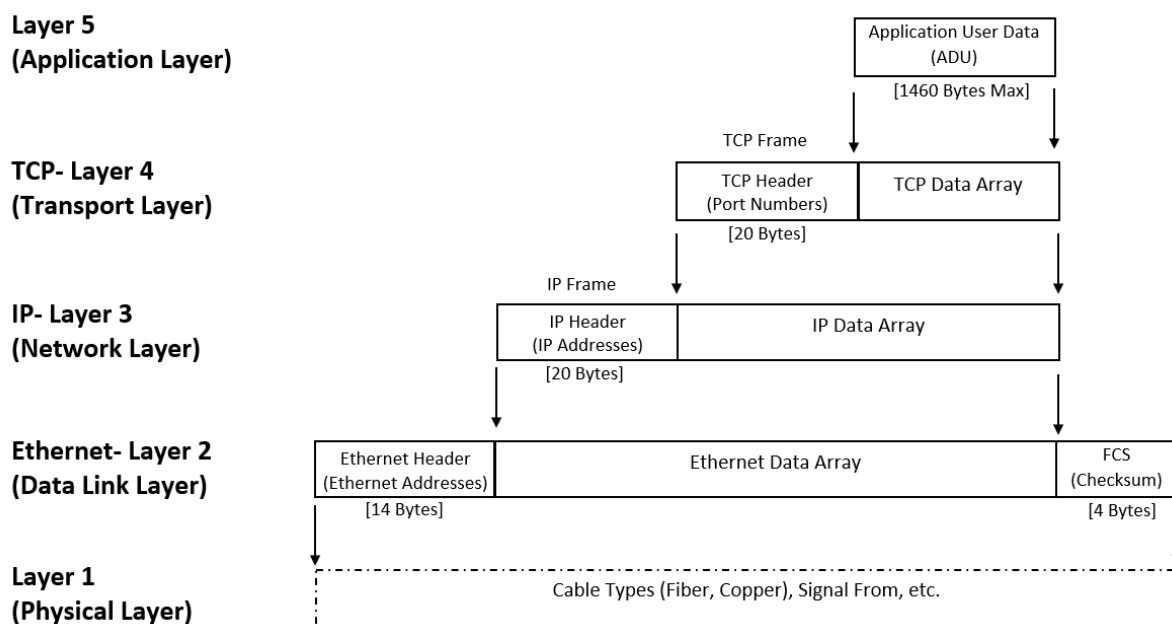


Figure 4- 9- OSI Model for TCP/IP Ethernet Data Packet

Schneider Automation have a Modbus Messaging Implementation Guide which summarizes a modified protocol for TCP/IP usage [24].

#### 4.5.1.1- Modbus Messaging on TCP/IP

Client/Server communication among devices is reinforced by the Modbus messaging service. The devices are connected on an Ethernet TCP/IP network. The following four type of messages are the basis for this client / server model [8]:

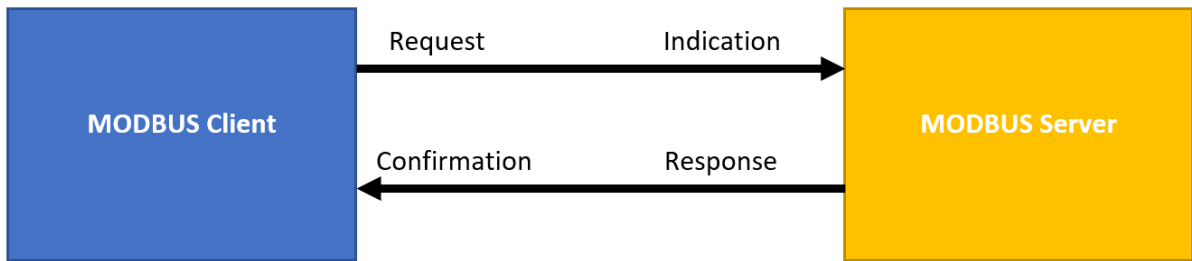


Figure 4- 10- Client-Server Messaging Model

- **Modbus Request** initiates the transaction which is sent by the Client.
- **Modbus Confirmation** confirms to the Client the message has been received.
- **Modbus Indication** is the message request that arrives on the Server side,
- **Modbus Response** is the message which the Server sends as a response.

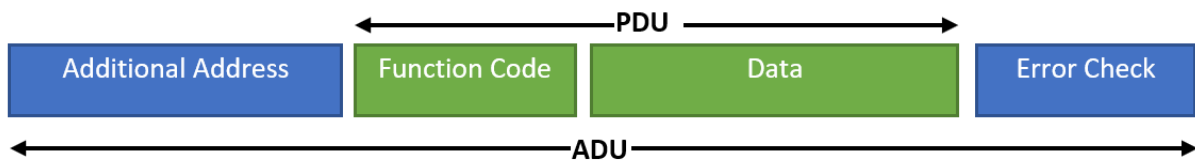


Figure 4- 11- General Modbus Frame

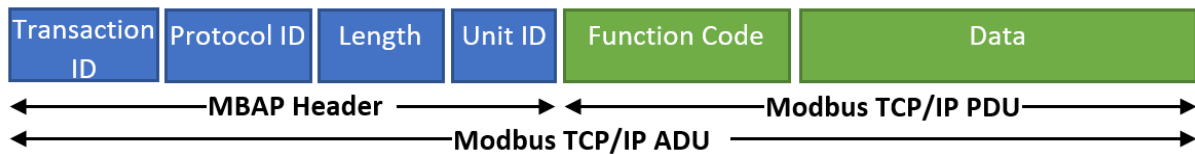


Figure 4- 12- Modbus Request/Response over TCP/IP

| Field          | Length  | Description   |
|----------------|---------|---|
| Transaction ID | 2 Bytes | used for transaction pairing, the Modbus server copies in the response the transaction identifier of the request  |
| Protocol ID    | 2 Bytes | used for intra-system multiplexing. The Modbus protocol is identified by the value 0  |
| Length         | 2 Bytes | count of the following fields, including the Unit Identifier and data fields  |
| Unit ID        | 1 Byte  | used for intra-system routing purpose. "It is typically used to communicate to a Modbus+ or a Modbus serial line slave through a gateway between an Ethernet TCP-IP network and a Modbus serial line" [8]. Unit ID is defined in the request by the Modbus Client. The server should return in the response the same value. |

Table 4- 1- MBAP Header Fields Description

Figure 4-11 describes the general Modbus Frame. A PDU which is separate from the underlying communication layer is determined by the Modbus protocol. The Modbus

protocol can also create specific mapping on buses or networks which can include some extra fields on the Application Data Unit (ADU).

The Modbus Application Data Unit is built by the Modbus transaction which the client activates. The server is then told what action is to be performed which is specified by the function code. Figure 4-12 describes the Modbus Request/Response Application Data Unit on a TCP/IP Network.

A specific header called MBAP header (Modbus Application Protocol header) is applied on TCP/IP to identify the Modbus Application Data Unit. Table 4-1 summarizes the contained fields [8].

The Modbus device provides a Client and/or a Server Modbus Interface. This interface may consist of four areas: input discrete, output discrete (coils) input registers and output registers. There is always a pre-mapping between the interface and the user application data that has to be done.

| Primary Tables    | Object Type | Type       | Description                                |
|-------------------|-------------|------------|--|
| Discretes Input   | Single Bit  | Read-Only  | Can be provided by an I/O system           |
| Coils             | Single Bit  | Read-Write | Can be alterable by an application program |
| Input Registers   | 16-Bit Word | Read-Only  | Can be provided by an I/O system           |
| Holding Registers | 16-Bit Word | Read-Write | Can be alterable by an application program |

*Table 4- 2- Areas of Modbus Interface*

#### 4.5.1.2- Modbus Components

**Modbus Client** permits the user application to regulate information transfers with a remote device. A Modbus request is created by the Modbus Client from parameters sent by the user application to the Modbus Client Interface. A Modbus transaction is used which holds the waiting and processing of a Modbus confirmation.

**Modbus Client Interface** presents an uncomplicated and accessible interface which supports the user application to design the requests for diverse Modbus services such as the access to Modbus application objects.

**Modbus Server** is on reception of a Modbus Request to activate an action, e.g. read or write. These processes are completely transparent for the application programmer. The primary functions of the Modbus server are the waiting for the Modbus request on the 502 TCP port, the treatment of the request and afterwards the building of the Modbus response according to the device context.

# 5

## Prototype Implementation

### 5.1- Test Setup

As explained in the last chapter, for implementing the possibility of testing the smart grids network in parallel to smart metering network, a test system with three Siemens one-phase smart meters [IM150] and a Data Gateway (DG) [SGW1050] implemented, as Fig. 5-1 and 5-2 showcases the real and schematic view of test system.

This prototype can work with any kind (different smart meter manufacturers) of smart meters which supports G3-PLC protocol. This is also applicable for the data gateway.

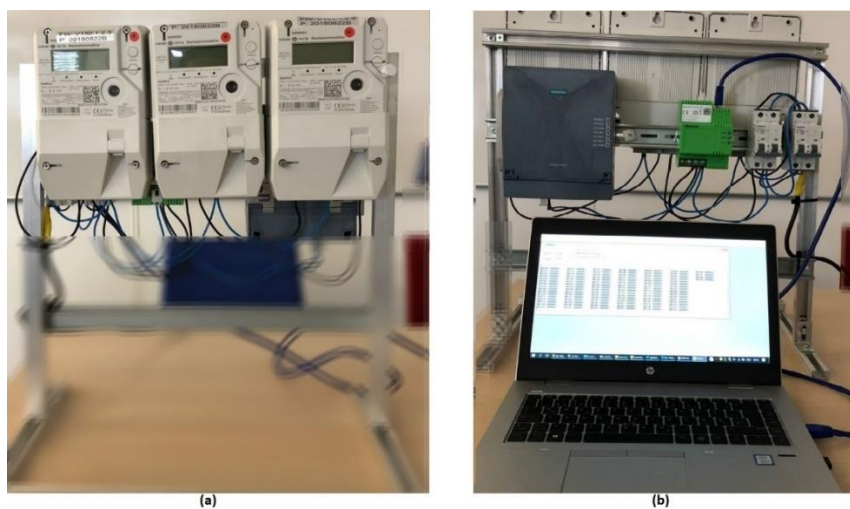


Figure 5- 1- Real Test System Structure- (a): Smart Meter Side, (b): Data Gateway Side

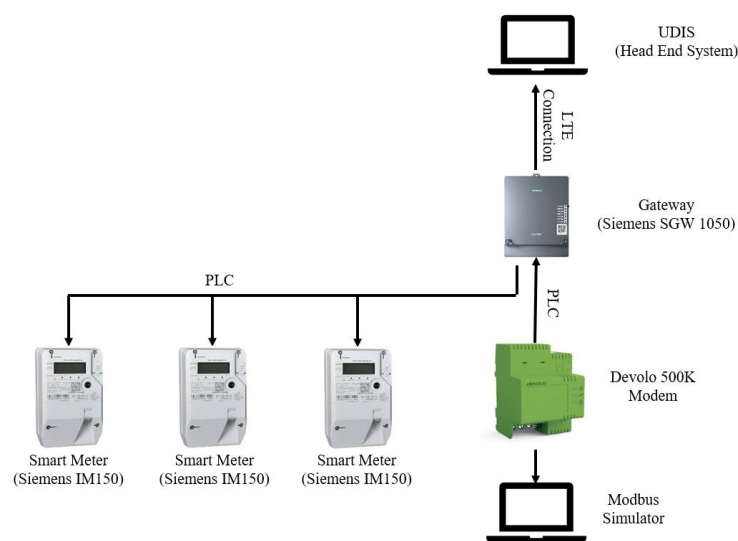


Figure 5- 2- Test System Schematic Structure

This test has been done in these conditions:

- In FCC frequency band and as a result almost a noise-free environment
- The communication is tested through only three smart meters, all in Hop-0
- A short wire between DG and measuring point that prevent from possible noises and disturbances.

As can be seen in figure 5-3, the start page of DG-Application user interface shows the number joined devices (Client), the LTE communication and other useful informations.



Figure 5- 3- DG-Application User Interface

All the PLC devices that have a data communication with the DG should be joined. Figure 5-4 showcases the joined devices. The Devolo 500K Modem is with the Node ID = 1 and the other Siemens Smart Meters are joined with Node IDs = 2, 3 and 5.

| PLC Devices      |         |        |                     |                 |          |      |                     |          |
|------------------|---------|--------|---------------------|-----------------|----------|------|---------------------|----------|
| EUI 64           | Node ID | Status | Anmelde Zeitpunkt   | Anmeldeversuche | Qualität | Pfad | Anfrage Zeit        | Aktion   |
| 30D32DFFFE45693A | 1       | joined | 12.03.2020 06:39:25 | 32              | 10       | 1    | 12.03.2020 06:37:46 | Wählen ▼ |
| 386E21FFFE7A1280 | 2       | joined | 12.03.2020 07:46:39 | 11              | 10       | 2    | 12.03.2020 06:37:46 | Wählen ▼ |
| 386E21FFFE7A1286 | 3       | joined | 12.03.2020 06:38:03 | 51              | 10       | 3    | 12.03.2020 06:37:46 | Wählen ▼ |
| 386E21FFFE7A128E | 5       | joined | 12.03.2020 06:38:06 | 55              | 10       | 5    | 12.03.2020 06:37:46 | Wählen ▼ |

Figure 5- 4- Joined Devices on DG

To make the smart grids communication possible, with the help of Devolo 500K Modem and Modbus Simulator a separate communication channel is built from the DG to Modbus Simulator (works as an assumed Measuring Point). This modem is responsible for delivering the IP packets to the DG.

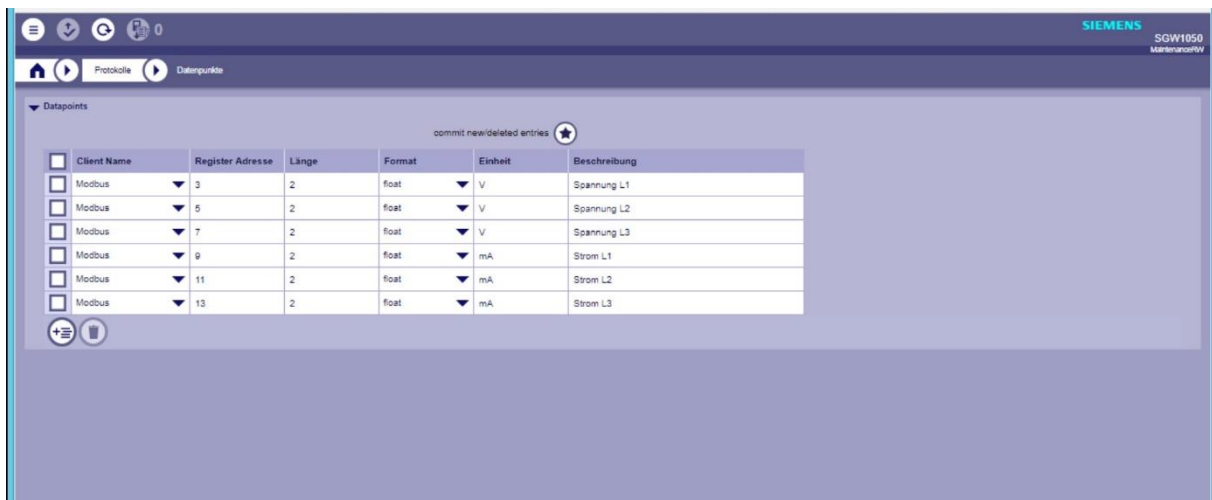
The Devolo 500K Modem is a router that take the packets and transfer them to the further interface. At one side G3-PLC and at the other side operates through Modbus because of IPv6 address or IP.



As the functionality of Modbus TCP/IP protocol explained in 4.4.1, Data Gateway acts also as a Modbus master and different data points (Modbus holding registers), as figure 5-5 showcases, are in DG-Application defined. These defined holding registers also, as figure 5-6 showcases, are in Modbus Simulator defined.

The data from Modbus Simulator are through Devolo modem to the DG every ten mSec transferred. As it is showed in the figures, six holding registers (three registers each for assumed three phase voltage and current) are defined.

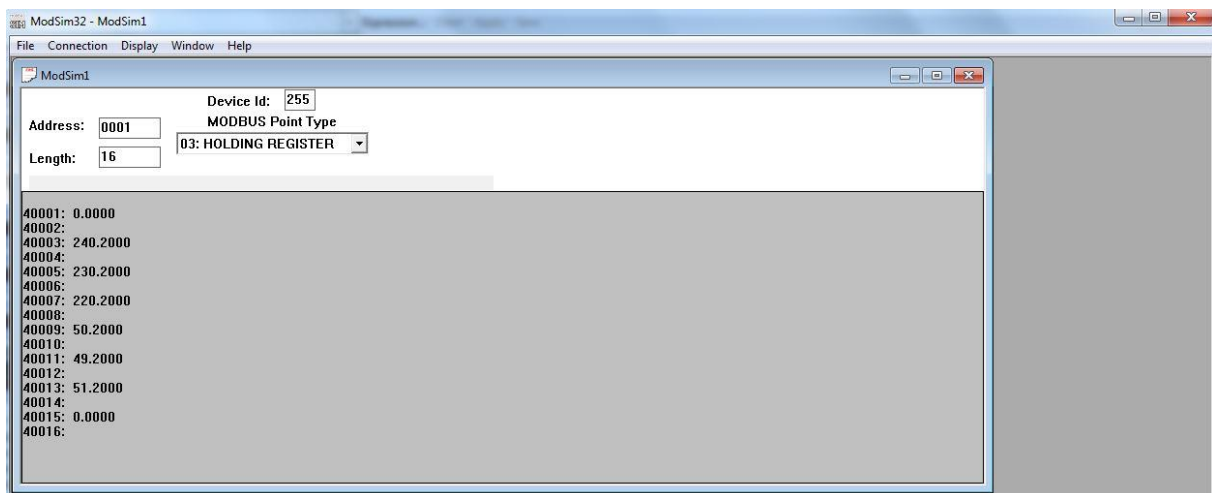
The idea for using this modem for transferring Modbus packets to DG, is that to simulate smart grids functionality by sending data packets continuously, like heart beats.



The screenshot shows the 'Datapoints' configuration window in the Siemens SGW1050 Maintenance RW software. It displays a table of six defined Modbus holding registers. Each register is associated with a specific data point description, such as 'Spannung L1' (Voltage L1) and 'Strom L1' (Current L1).

| Client Name | Register Adresse | Länge | Format | Einheit | Beschreibung |
|-------------|------------------|-------|--------|---------|--------------|
| Modbus      | 3                | 2     | float  | V       | Spannung L1  |
| Modbus      | 5                | 2     | float  | V       | Spannung L2  |
| Modbus      | 7                | 2     | float  | V       | Spannung L3  |
| Modbus      | 9                | 2     | float  | mA      | Strom L1     |
| Modbus      | 11               | 2     | float  | mA      | Strom L2     |
| Modbus      | 13               | 2     | float  | mA      | Strom L3     |

Figure 5- 5- Data Points (Modbus Holding Registers) defined for DG



The screenshot shows the 'ModSim1' configuration window in the ModSim32 - ModSim1 software. It displays the configuration for a Modbus device with ID 255. The 'MODBUS Point Type' is set to '03: HOLDING REGISTER'. Below the configuration fields, a list of 16 registers is shown, each with its address and a numerical value.

| Address | Value    |
|---------|----------|
| 40001:  | 0.0000   |
| 40002:  |          |
| 40003:  | 240.2000 |
| 40004:  |          |
| 40005:  | 230.2000 |
| 40006:  |          |
| 40007:  | 220.2000 |
| 40008:  |          |
| 40009:  | 50.2000  |
| 40010:  |          |
| 40011:  | 49.2000  |
| 40012:  |          |
| 40013:  | 51.2000  |
| 40014:  |          |
| 40015:  | 0.0000   |
| 40016:  |          |

Figure 5- 6- Data Points (Modbus Holding Registers) defined for Modbus Simulator

As can be seen in Figure 5-7, after a communication established, the values are correctly transmitted to DG.

| Datapoint ID               | Timestamp               | Data Type | Value             | Unit | Quality | Cause of Trans... |
|----------------------------|-------------------------|-----------|-------------------|------|---------|-------------------|
| Modbus.register.holding.3  | 2020-03-12 09:15:28.273 | FLOAT     | 240.1999999432... | V    | GOOD    | SPONTANEOUS       |
| Modbus.register.holding.7  | 2020-03-12 09:15:28.754 | FLOAT     | 220.8000030517... | V    | GOOD    | SPONTANEOUS       |
| Modbus.register.holding.5  | 2020-03-12 09:15:28.478 | FLOAT     | 230.1999999432... | V    | GOOD    | SPONTANEOUS       |
| Modbus.register.holding.9  | 2020-03-12 09:15:29.050 | FLOAT     | 50.20000076293... | mA   | GOOD    | SPONTANEOUS       |
| Modbus.register.holding.11 | 2020-03-12 09:15:29.275 | FLOAT     | 49.20000075293... | mA   | GOOD    | SPONTANEOUS       |
| Modbus.register.holding.13 | 2020-03-12 09:15:29.490 | FLOAT     | 51.0              | mA   | GOOD    | SPONTANEOUS       |

Figure 5- 7- Transferred Values from Modbus Simulator to DG

To implement the smart metering functionality, a spontaneous read-out of meter data, as figure 5-8 showcases, is established every ten minutes through UDIS HES.

| Seriesnummer     | Zählernummer | Gateway      | Hess-Profil-Name | Technische Daten |
|------------------|--------------|--------------|------------------|------------------|
| SHS1020788000128 | IM150-AIC10P | DP1170000050 | IM150_SE         | Technische Daten |
| SHS1020788000134 | IM150-AIC10P | DP1170000050 | IM150_SE         | Technische Daten |
| SHS1020788000142 | IM150-AIC10P | DP1170000050 | IM150_SE         | Technische Daten |

Figure 5- 8- Spontaneous Read-Out of meter data through UDIS HES

To analyze signals and telegrams, there is the possibility to have running messages between DG and Smart Meter with the arrival/send time to/from DG-Application with the help of Internet Control Message Protocol (ICMP) in a csv File. The time stamps for this analyze are with a delay in compare to real time since the reference would be the arrival/send time in DG-Application. Also, to analyze the signals with considering of the packet lost, a nBox (Neuron Box) of the company Neuron is installed. This sniffer is responsible to record the packets of LV communication in the nBox as a wireshark file (Figure 5-9).

| Folder              | Size    | #pkts | Start/End time                             |
|---------------------|---------|-------|--|
| PLC_Modbus_1 pcap00 | 9.54M   | 45296 | 28.02.2020 09:42:11<br>28.02.2020 12:36:55 |
| PLC_Modbus_1 pcap01 | 449.23K | 2173  | 28.02.2020 12:37:00<br>28.02.2020 15:21:57 |
| PLC_Modbus_2 pcap   | 9.54M   | 37290 | 12.03.2020 07:42:38<br>12.03.2020 11:24:21 |
| PLC_Modbus_2 pcap01 | 6.05M   | 23356 | 12.03.2020 11:24:21<br>12.03.2020 12:29:57 |

Figure 5- 9 - Wireshark Files nBox

Because the packets are encrypted, in the Siemens DG a lab-firmware is installed in order to make the readout of the AES-Key for the LV communication possible. This AES-Key is in the nBox recorded. In this way the packets are available in plain text (Figure 5-10).

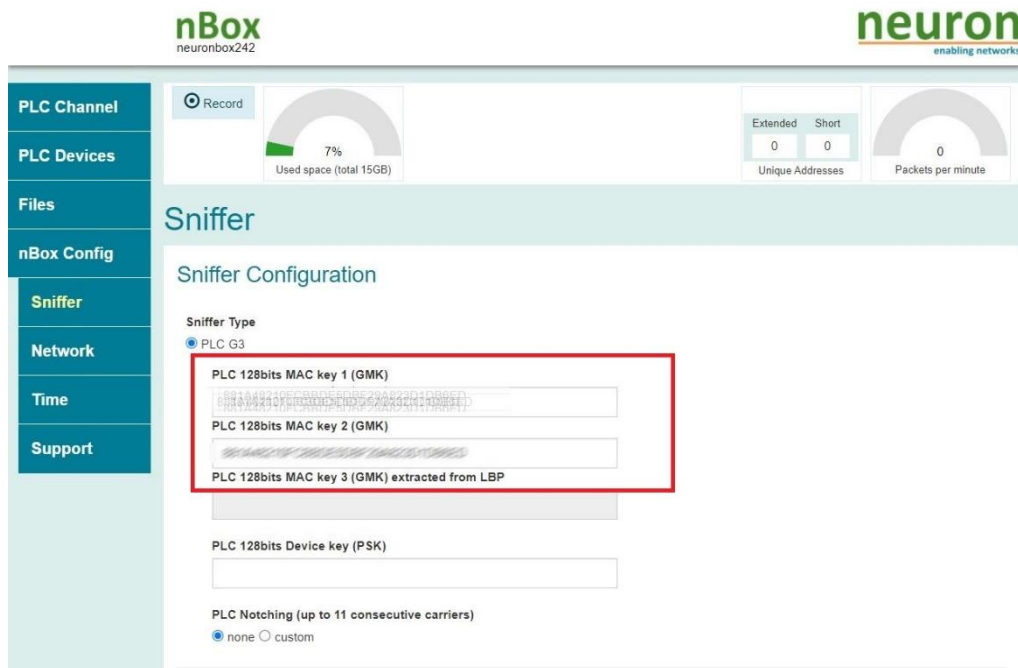


Figure 5- 10- AES Key for nBox

Figure 5-11 showcases the typical sequence of telegrams in MAC-Layer. Both for a same packet, Figure 5-10 (a) shows from the csv file with the time stamp from DG-Application and 5-10 (b) from wireshark file. As it is clear, the times in both figures are with one-hour difference. It should mention that the time stamps in DG-Application are in UTC-Time and the time stamps in wireshark file is the local time in Vienna.

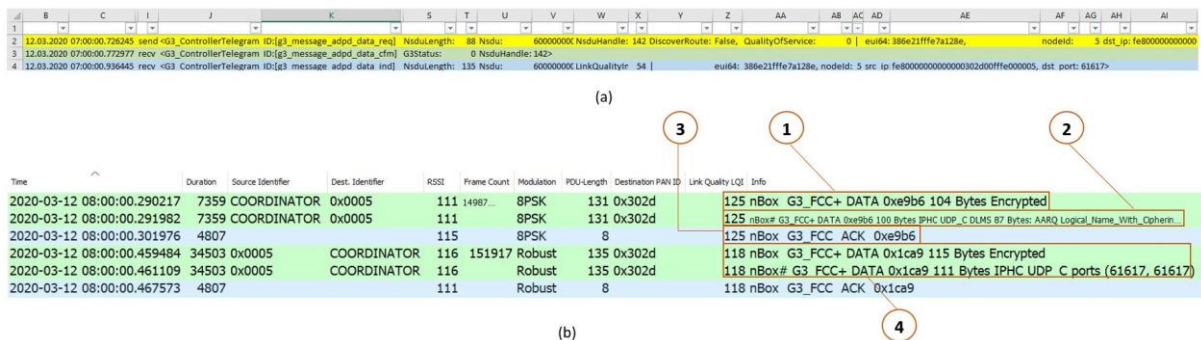


Figure 5- 11- Outline of Telegram Packet in (a) Wireshark and (b) DG-Application

Coordinator (DG) sends a telegram [Data\_Req] to Smart Meter. The modulation process used is 8PSK. The packet has the PSDU length of 131-byte and a 104-byte payload length (1). Because of the AES-Key for the MAC-Encryption, that is in the nBox recorded, the decrypted telegram [nBox#] can in plain text represented. Since the packet deals with nBox, and not a packet that in the LV communication transferred, it is marked with the hashtag in nBox (2). The checksum of MAC-Data is 0xe9b6 and sent in the next ACK-Telegram as an identification (3). The smart meter replies to Data\_Req and sends a Data\_Ind.

## 5.2- Application Method

For the test series, two test series, with each lasting for two hours are planned. The first series is for testing the functionality of smart metering and the second round is for testing the functionality of smart grids communication in parallel with smart metering with the help of Devolo 500K modem and Modbus Simulator. The first goal is to check the possibility of this connection and next to see how the functionality of smart metering changes with the emerge of smart grids data packets. In this case a two-hours time window can fulfill our expectations for analyzing.

The relevant time stamps are saved in DG in a Diagnosis File. To analyze these data, a csv File is generated from diagnosis file, that gives us an overall overview of communication between smart meters and DG.

Figure 5-12 showcases two types of evaluating time values:

- *ackDelta* the difference time of sending the packet from DG in MAC-Level until an ACK in MAC-Side arrived from smart meter.
- *rspDelta* the difference time of sending the packet from DG in MAC-Level until an Echo-Reply in MAC-Side arrived from smart meter.

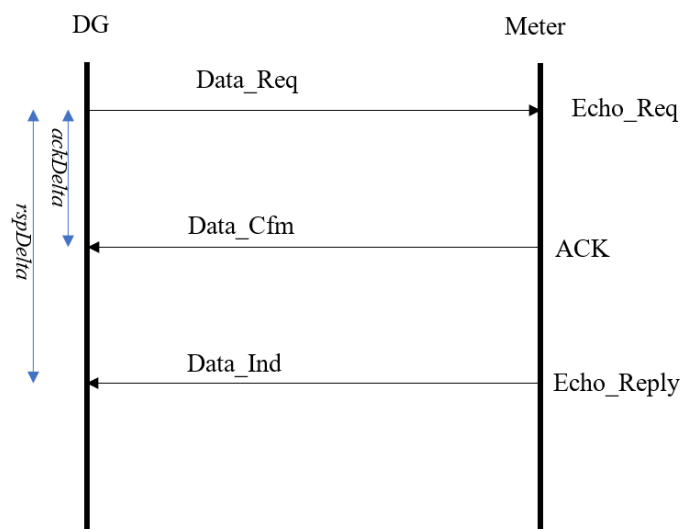


Figure 5- 12- Time calculation in DG-Application

## 5.2.1- Calculation of Reaction Times

Through comparing of *ackDelta* and *rspDelta* as two main criteria for calculation of reaction time in both situations, we can have an overall overview of how the reaction times in case of smart grids change and increases. Table 5-1 showcases these reaction times.

| Test Serie     | ackDelta [mSec] | rspDelta [mSec] | Number of Telegrams |
|----------------|-----------------|-----------------|---------------------|
| Smart Metering | 55,4836         | 172,5154        | 598                 |
| Smart Grids    | 61,8834         | 191,577         | 467                 |

*Table 5- 1- Analyze of reaction time based on the telgerams arrived in DG-Application*

As we can see, both reaction times in smart grids test serie in compare to smart metering test serie increase and number of telegrams decrease, that is because of arriving more smart grids packets in between.

As explained, the nBox sniffers the LV communication signals. In this case we have the opportunity to see and analyze the signals, the possible packet lost, and also the signals send from Devolo modem. Table 5-2 and 5-3 showcase the reaction times for smart metering and smart grids test series respectively.

|                |                 |         |                          |
|----------------|-----------------|---------|--------------------------|
| Smart Metering | ackDelta [mSec] | 10,842  | Number of Telegrams: 673 |
|                | rspDelta [mSec] | 109,076 | Number of Telegrams: 661 |

*Table 5- 2- Analyze of reaction times of smart metering test serie based on the telgerams arrived in nBox*

|                |                |                 |         |                           |
|----------------|----------------|-----------------|---------|---------------------------|
| Smart<br>Grids | Smart<br>Meter | ackDelta [mSec] | 10,889  | Number of Telegrams: 467  |
|                |                | rspDelta [mSec] | 121,265 | Number of Telegrams: 460  |
|                | Modbus         | ackDelta [mSec] | 8,826   | Number of Telegrams: 9764 |
|                |                | rspDelta [mSec] | 121,541 | Number of Telegrams: 5521 |

*Table 5- 3- Analyze of reaction times of smart grids test serie based on the telgerams arrived in nBox*

Analyzing Table 5-2 and 5-3 show us that in smart grids test serie in compare to smart metering test serie, less telegrams have the chance to communicate between DG and smart meter. In this case the average *rspDelta* time increases. Another reason for less telegrams in smart grids test serie for communication of smart meters is that huge amount of Devolo modem telegrams causes more packet lost for delivery of smart meter data packets in smart grids network.

## 5.2.2- Signal Lifespan

Figure 5-13 showcases a signal lifespan from the time a REQ telegram is sent and the RSP telegram arrives with their equivalent ACK telegram.

In the signal lifespan we have a new criterion that we call  $\Delta SW$  as software processing time. The  $\Delta SW$  is calculated through (1) and composed of two parts:

$$\Delta SW = \Delta SW_{ack} + \Delta SW_{rsp} \quad (1)$$

- $\Delta SW_{ack}$  is the time interval between sending a telegram and sending of the related ACK Telegram. In G3-PLC standard this time gap is predefined and described as inter-frame (IFS) spacing [10, P. 54]
- $\Delta SW_{rsp}$  is the time interval between receiving an ACK and sending of the next Telegram.

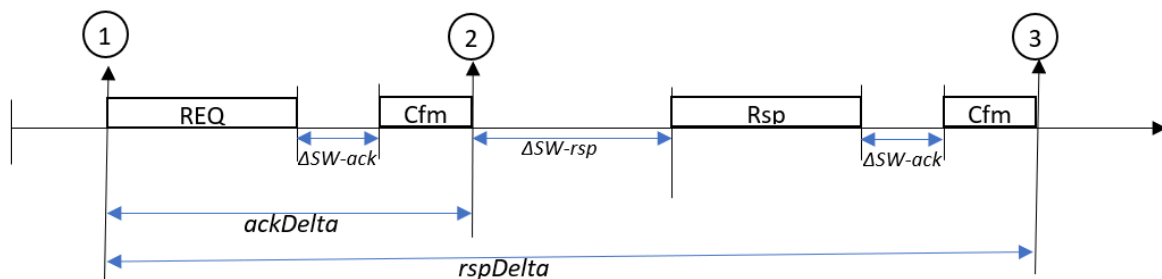


Figure 5- 13- Signal Lifespan

According to G3-PLC standard,  $\Delta SW_{ack}$  is already defined and the network cannot send another telegram during this time interval, but it is possible because of the communication traffic, during the time gap of  $\Delta SW_{rsp}$ , different telegrams from other devices come in between and as a result causes the increase of  $rspDelta$ . As an example figure 5-14 showcases that DG sends a telegram to 0x0002 (1), in the meantime Devolo modem (LVL0\_Device1) communicates with DG (2), after that 0x0002 replies to the DG with a delay (3). This extra telegrams between DG and Devolo Modem (because of smart grids functionality) caused a  $rspDelta$  time for 0x0002 to be 443,803 mSec that is far longer than average time (121 mSec).

| Time                       | Duration | Source Identifier | Dest. Identifier | RSSI | Frame Count | Modulation | POU Length | Destination PAN ID | Link Quality LQI | POU length (symbols) | Info   |
|----------------------------|----------|-------------------|------------------|------|-------------|------------|------------|--------------------|------------------|----------------------|--|
| 2020-03-12 10:25:07.785732 | 5967     | COORDINATOR       | 0x0002           | 111  | 14989672    | 8PSK       | 50         | 0x302d             | 142              | 26                   | nBox G3_FCC+ DATA 0xf089 30 Bytes Encrypted                        |
| 2020-03-12 10:25:07.787283 | 5967     | COORDINATOR       | 0x0002           | 111  |             | 8PSK       | 50         | 0x302d             | 142              | 26                   | nBox# G3_FCC+ DATA 0xf089 26 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:07.796263 | 4807     |                   |                  | 117  |             | 8PSK       | 8          |                    | 142              | 21                   | nBox G3_FCC ACK 0xf089   |
| 2020-03-12 10:25:07.837704 | 29631    | COORDINATOR       | Lvl0_Device1     | 111  | 14989673    | Robust     | 111        | 0x302d             | 125              | 128                  | nBox G3_FCC+ DATA 0x1359 91 Bytes Encrypted                        |
| 2020-03-12 10:25:07.839289 | 29631    | COORDINATOR       | Lvl0_Device1     | 111  |             | Robust     | 111        | 0x302d             | 125              | 128                  | nBox# G3_FCC+ DATA 0x1359 87 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:07.844545 | 4807     |                   |                  | 115  |             | Robust     | 8          |                    | 125              | 21                   | nBox G3_FCC ACK 0x1359   |
| 2020-03-12 10:25:07.931060 | 30095    | Lvl0_Device1      | COORDINATOR      | 114  | 1118        | Robust     | 113        | 0x302d             | 132              | 130                  | nBox G3_FCC+ DATA 0xda63 93 Bytes Encrypted                        |
| 2020-03-12 10:25:07.932676 | 30095    | Lvl0_Device1      | COORDINATOR      | 114  |             | Robust     | 113        | 0x302d             | 132              | 130                  | nBox# G3_FCC+ DATA 0xda63 89 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:07.939010 | 4807     |                   |                  | 111  |             | Robust     | 8          |                    | 132              | 21                   | nBox G3_FCC ACK 0xda63   |
| 2020-03-12 10:25:08.002009 | 27079    | COORDINATOR       | Lvl0_Device1     | 111  | 14989674    | Robust     | 99         | 0x302d             | 128              | 117                  | nBox G3_FCC+ DATA 0x36fe 79 Bytes Encrypted                        |
| 2020-03-12 10:25:08.003703 | 27079    | COORDINATOR       | Lvl0_Device1     | 111  |             | Robust     | 99         | 0x302d             | 128              | 117                  | nBox# G3_FCC+ DATA 0x36fe 75 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:08.008714 | 4807     |                   |                  | 115  |             | Robust     | 8          |                    | 128              | 21                   | nBox G3_FCC ACK 0x36fe   |
| 2020-03-12 10:25:08.045482 | 27079    | COORDINATOR       | Lvl0_Device1     | 111  | 14989675    | Robust     | 99         | 0x302d             | 127              | 117                  | nBox G3_FCC+ DATA 0x0cd9 79 Bytes Encrypted                        |
| 2020-03-12 10:25:08.047079 | 27079    | COORDINATOR       | Lvl0_Device1     | 111  |             | Robust     | 99         | 0x302d             | 127              | 117                  | nBox# G3_FCC+ DATA 0x0cd9 75 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:08.056377 | 4807     |                   |                  | 114  |             | Robust     | 8          |                    | 127              | 21                   | nBox G3_FCC ACK 0x0cd9   |
| 2020-03-12 10:25:08.121149 | 27311    | Lvl0_Device1      | COORDINATOR      | 114  | 1119        | Robust     | 100        | 0x302d             | 132              | 118                  | nBox G3_FCC+ DATA 0xf05c 80 Bytes Encrypted                        |
| 2020-03-12 10:25:08.122756 | 27311    | Lvl0_Device1      | COORDINATOR      | 114  |             | Robust     | 100        | 0x302d             | 132              | 118                  | nBox# G3_FCC+ DATA 0xf05c 76 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:08.128018 | 4807     |                   |                  | 111  |             | Robust     | 8          |                    | 132              | 21                   | nBox G3_FCC ACK 0xf05c   |
| 2020-03-12 10:25:08.183152 | 27311    | Lvl0_Device1      | COORDINATOR      | 115  | 1120        | Robust     | 100        | 0x302d             | 130              | 118                  | nBox G3_FCC+ DATA 0x1ec1 80 Bytes Encrypted                        |
| 2020-03-12 10:25:08.184931 | 27311    | Lvl0_Device1      | COORDINATOR      | 115  |             | Robust     | 100        | 0x302d             | 130              | 118                  | nBox# G3_FCC+ DATA 0x1ec1 76 Bytes IPHC UDP_C ports (9090, 9090)   |
| 2020-03-12 10:25:08.190091 | 4807     |                   |                  | 111  |             | Robust     | 8          |                    | 130              | 21                   | nBox G3_FCC ACK 0x1ec1   |
| 2020-03-12 10:25:08.221301 | 15943    | 0x0002            | COORDINATOR      | 115  | 206677      | Robust     | 45         | 0x302d             | 108              | 69                   | nBox G3_FCC+ DATA 0x99e4 25 Bytes Encrypted                        |
| 2020-03-12 10:25:08.222966 | 15943    | 0x0002            | COORDINATOR      | 115  |             | Robust     | 45         | 0x302d             | 108              | 69                   | nBox# G3_FCC+ DATA 0x99e4 21 Bytes IPHC UDP_C ports (61617, 61617) |
| 2020-03-12 10:25:08.229535 | 4807     |                   |                  | 111  |             | Robust     | 8          |                    | 108              | 21                   | nBox G3_FCC ACK 0x99e4   |

Figure 5- 14- Communication of other devices during  $\Delta SW_{rsp}$



## 5.2.3- Effects of Noises in the Overall Performance

Nowadays data communication among devices in an electrical grid can be done through PLC. Still some factors such as attenuation and noises of equipment can degrade the performance of the system [14].

In this test system, in the two hours test serie for smart grids, it is noticed that eight times a noise occurred in the system and significantly degraded the performance and caused delay in *rspDelta*.

As an example figure 5-15 showcases that DG and 0x0003 communicating with each other more times fast and efficient (1) with an average *rspDelta* of 121 mSec. But because of an unknown noise measured by nBox and also an unwanted DG-Request on devolo modem(2), smart meter 0x0003 replied to the DG with a delay. In this case the *rspDelta* for this telegram was 6,425 sec, that is a huge degrading of the overall performance of the system.

|                            |              |             |     |                 |            |     |  |
|----------------------------|--------------|-------------|-----|-----------------|------------|-----|--|
| 2020-03-12 11:35:23.277066 | 15943 0x0003 | COORDINATOR | 116 | 252842 Robust   | 45 0x302d  | 114 | 69 nBox G3_FCC+ DATA 0x0003 25 Bytes Encrypted   |
| 2020-03-12 11:35:23.278547 | 15943 0x0003 | COORDINATOR | 116 | Robust          | 45 0x302d  | 114 | 69 nBox G3_FCC+ DATA 0x0003 25 Bytes Encrypted   |
| 2020-03-12 11:35:23.287944 | 4807         |             | 111 | Robust          | 8          | 114 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:23.381344 | 6199 0x0003  | COORDINATOR | 111 | 14995653 BPJK   | 64 0x302d  | 122 | 27 nBox G3_FCC+ DATA 0x0003 49 Bytes Encrypted   |
| 2020-03-12 11:35:23.382026 | 6199 0x0003  | COORDINATOR | 111 | BPJK            | 64 0x302d  | 122 | 27 nBox G3_FCC+ DATA 0x0003 49 Bytes Encrypted   |
| 2020-03-12 11:35:23.393366 | 4807         |             | 116 | BPJK            | 8          | 122 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:23.734763 | 18959 0x0003 | COORDINATOR | 115 | 252842 Robust   | 59 0x302d  | 112 | 82 nBox G3_FCC+ DATA 0x0003 39 Bytes Encrypted   |
| 2020-03-12 11:35:23.736417 | 18959 0x0003 | COORDINATOR | 115 | Robust          | 59 0x302d  | 112 | 82 nBox G3_FCC+ DATA 0x0003 39 Bytes Encrypted   |
| 2020-03-12 11:35:23.742988 | 4807         |             | 111 | Robust          | 8          | 112 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:24.198418 | 7359 0x0003  | COORDINATOR | 111 | 14995658 BPJK   | 131 0x302d | 143 | 32 nBox G3_FCC+ DATA 0x0003 194 Bytes Encrypted  |
| 2020-03-12 11:35:24.201567 | 7359 0x0003  | COORDINATOR | 111 | BPJK            | 131 0x302d | 143 | 32 nBox G3_FCC+ DATA 0x0003 194 Bytes Encrypted  |
| 2020-03-12 11:35:24.209351 | 4807         |             | 115 | BPJK            | 8          | 143 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:24.368924 | 34503 0x0003 | COORDINATOR | 115 | 252844 Robust   | 135 0x302d | 115 | 149 nBox G3_FCC+ DATA 0x0003 115 Bytes Encrypted |
| 2020-03-12 11:35:24.370586 | 34503 0x0003 | COORDINATOR | 115 | Robust          | 135 0x302d | 115 | 149 nBox G3_FCC+ DATA 0x0003 115 Bytes Encrypted |
| 2020-03-12 11:35:24.750535 | 4807         |             | 111 | Robust          | 8          | 115 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:24.759593 | 6663 0x0003  | COORDINATOR | 111 | 14995657 BPJK   | 91 0x302d  | 108 | 29 nBox G3_FCC+ DATA 0x0003 88 Bytes Encrypted   |
| 2020-03-12 11:35:24.766697 | 6663 0x0003  | COORDINATOR | 111 | BPJK            | 91 0x302d  | 108 | 29 nBox G3_FCC+ DATA 0x0003 88 Bytes Encrypted   |
| 2020-03-12 11:35:24.807913 | 4807         |             | 115 | BPJK            | 8          | 108 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:24.807913 | 28703 0x0003 | LvB_Device1 | 111 | 14995658 Robust | 107 0x302d | 129 | 124 nBox G3_FCC+ DATA 0x0003 87 Bytes Encrypted  |
| 2020-03-12 11:35:24.807913 | 28703 0x0003 | LvB_Device1 | 111 | Robust          | 107 0x302d | 129 | 124 nBox G3_FCC+ DATA 0x0003 87 Bytes Encrypted  |
| 2020-03-12 11:35:24.807913 | 4807         |             | 115 | Robust          | 8          | 129 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:24.807913 | 23135 0x0003 | COORDINATOR | 114 | 252843 Robust   | 80 0x302d  | 113 | 100 nBox G3_FCC+ DATA 0x0003 69 Bytes Encrypted  |
| 2020-03-12 11:35:24.807913 | 23135 0x0003 | COORDINATOR | 114 | Robust          | 80 0x302d  | 113 | 100 nBox G3_FCC+ DATA 0x0003 69 Bytes Encrypted  |
| 2020-03-12 11:35:24.807913 | 4807         |             | 116 | Robust          | 8          | 113 | 21 nBox G3_FCC+ ACK 0x0003                       |
| 2020-03-12 11:35:24.807913 | 28935 0x0003 | COORDINATOR | 115 | 4343 Robust     | 108 0x302d | 130 | 125 nBox G3_FCC+ DATA 0x0003 88 Bytes Encrypted  |
| 2020-03-12 11:35:24.807913 | 28935 0x0003 | COORDINATOR | 115 | Robust          | 108 0x302d | 130 | 125 nBox G3_FCC+ DATA 0x0003 88 Bytes Encrypted  |
| 2020-03-12 11:35:24.807913 | 4807         |             | 111 | Robust          | 8          | 130 | 21 nBox G3_FCC+ ACK 0x0003                       |

Figure 5- 15- Effects of Noises in the Overall Performance

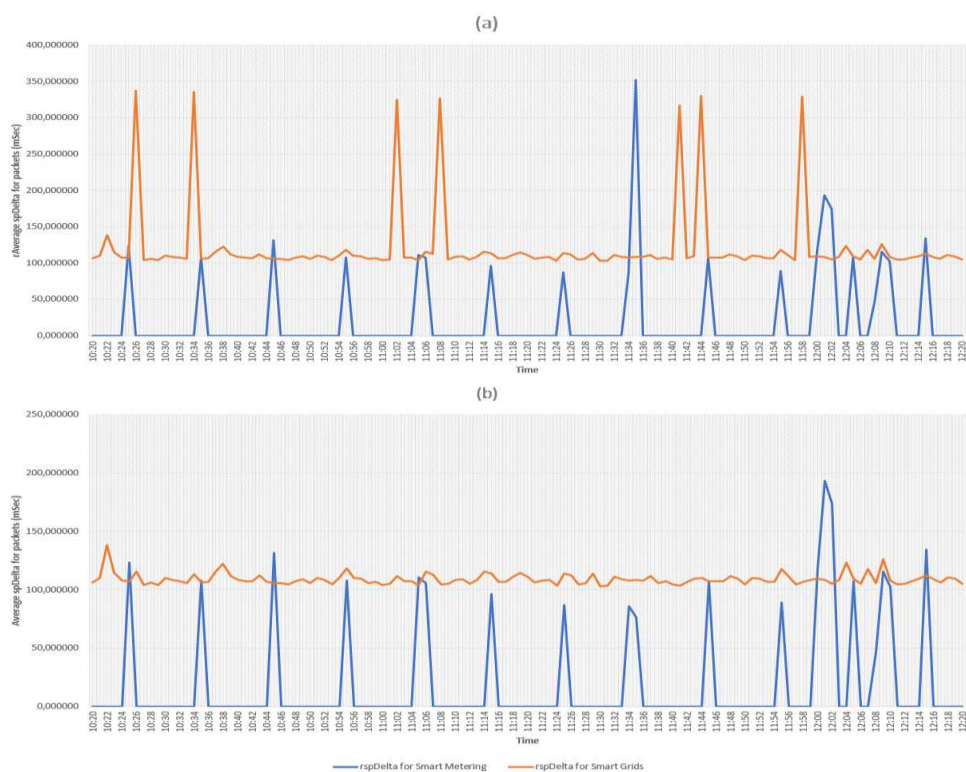


Figure 5- 16- Average *rspDelta* in every minute in the Smart Grids Test Serie  
(a) real (b) in the absence of background noises



To figure out, how the noises can affect the overall performance of the system and also to show how the noises can heavily affect the increasing of reaction times, in the whole two hours of smart grids test serie, eight massive background noises are detected that caused a delay in *rspDelta* from 6 to 11 seconds. Figure 5-16- (a) showcases the average *rspDelta* in every minute for smart meters and Devolo data packets. In compare Figure 5-16- (b) showcases how the average *rspDelta* in every minute would be improved in the absence of background noises.

## 5.2.4- Effects of Joining Process in the Overall Performance

During the test serie, it can happen because of unknown communication problems, the response from smart meter does not arrive and as a result the joining status of a meter is lost and DG tries to connect to the meter again with running a RREQ repair.

As figure 5-17 showcases, after emerging noises (1), in response to a broadcast message, all the devices answers except 0x0002(2). The DG runs a JOINING process (3) and then a RREQ repair (4). This whole process lasts around 12 seconds, that causes in degrading the overall response time of the system.

| Time                       | Duration | Source Identifier                      | Dest. Identifier     | RSS | Frame Count   | Modulation | PSDU Length | Destination Pk ID | Link Quality LQI | PSDU length (symbols) | Info  |
|----------------------------|----------|--|----------------------|-----|---------------|------------|-------------|-------------------|------------------|-----------------------|---|
| 2020-03-12 08:47:22.556072 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:27.358277 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:32.411975 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:37.359807 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:42.362517 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:47.361968 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:52.361912 |          |  |                      |     |               |            |             |                   |                  |                       | noise NOISE MEASUREMENT: AVG=00, NBL_POS=00, MAX=00 @ 75.00 kHz                       |
| 2020-03-12 08:47:53.080318 |          | 1947                                   | BROADCAST            | 115 | Robust        | 13 Gsmf    | 96          |                   |                  |                       | 41 noise G3_FCC 0x0003 1 Bytes BCH REQ  |
| 2020-03-12 08:47:54.877772 |          | 10375 COORDINATOR                      |                      | 111 | Robust        | 18         | 130         |                   |                  |                       | 45 noise G3_FCC 0x0003 6 Bytes BCH PkID C   |
| 2020-03-12 08:47:55.733442 |          | 10375 0x0003                           |                      | 116 | Robust        | 18         | 107         |                   |                  |                       | 45 noise G3_FCC 0x0003 6 Bytes BCH COST 12  |
| 2020-03-12 08:47:57.363606 |          | 10375 Lnk_Opical                       |                      | 115 | Robust        | 18         | 121         |                   |                  |                       | 45 noise G3_FCC 0x0003 6 Bytes BCH COST 12  |
| 2020-03-12 08:48:02.142345 |          | 10375 0x0003                           |                      | 115 | Robust        | 18         | 110         |                   |                  |                       | 45 noise G3_FCC 0x0003 6 Bytes BCH COST 12  |
| 2020-03-12 08:48:05.024554 |          | 12391 38-6e-21-ff-7e-12-80 COORDINATOR |                      | 117 | Robust        | 32 0x302d  | 109         |                   |                  |                       | 58 noise G3_FCC+DATA 0x002f 12 Bytes LBP (VasienGr)FFFF7A1280 JOINING                 |
| 2020-03-12 08:48:05.031029 |          | 4807                                   |                      | 111 | Robust        | 8          | 159         |                   |                  |                       | 21 noise G3_FCC ACK 0x002f  |
| 2020-03-12 08:48:05.132260 |          | 13623 COORDINATOR                      | 38-6e-21-ff-7e-12-80 | 111 | Robust        | 34 0x302d  | 128         |                   |                  |                       | 59 noise G3_FCC+ 0x0009 13 Bytes THL_FCC MOD_Robust TONES_ffff LQI 58                 |
| 2020-03-12 08:48:05.141774 |          | 4807                                   |                      | 116 | Robust        | 8          | 128         |                   |                  |                       | 21 noise G3_FCC ACK 0x0009  |
| 2020-03-12 08:48:05.204642 |          | 19423 COORDINATOR                      | 38-6e-21-ff-7e-12-80 | 111 | Robust        | 62 0x302d  | 128         |                   |                  |                       | 84 noise G3_FCC+DATA 0x0099 42 Bytes LBP (VasienGr)FFFF7A1280 CHALLENGE EAPReq(mes1)  |
| 2020-03-12 08:48:05.210628 |          | 4807                                   |                      | 117 | Robust        | 8          | 128         |                   |                  |                       | 21 noise G3_FCC ACK 0x0099  |
| 2020-03-12 08:48:05.267910 |          | 26151 38-6e-21-ff-7e-12-80 COORDINATOR |                      | 117 | Robust        | 94 0x302d  | 106         |                   |                  |                       | 113 noise G3_FCC+DATA 0x0001 74 Bytes LBP (VasienGr)FFFF7A1280 JOINING EAPReq(mes2)   |
| 2020-03-12 08:48:05.254183 |          | 4807                                   |                      | 111 | Robust        | 8          | 106         |                   |                  |                       | 21 noise G3_FCC ACK 0x0001  |
| 2020-03-12 08:48:05.410167 |          | 31923 COORDINATOR                      | 38-6e-21-ff-7e-12-80 | 111 | Robust        | 118 0x302d | 125         |                   |                  |                       | 124 noise G3_FCC+DATA 0x000d 98 Bytes LBP (VasienGr)FFFF7A1280 CHALLENGE EAPReq(mes3) |
| 2020-03-12 08:48:05.418476 |          | 4807                                   |                      | 117 | Robust        | 8          | 125         |                   |                  |                       | 21 noise G3_FCC ACK 0x000d  |
| 2020-03-12 08:48:05.450494 |          | 23135 38-6e-21-ff-7e-12-80 COORDINATOR |                      | 117 | Robust        | 80 0x302d  | 107         |                   |                  |                       | 100 noise G3_FCC+DATA 0x00ab 60 Bytes LBP (VasienGr)FFFF7A1280 JOINING EAPReq(mes4)   |
| 2020-03-12 08:48:05.450494 |          | 4807                                   |                      | 111 | Robust        | 8          | 107         |                   |                  |                       | 21 noise G3_FCC ACK 0x00ab  |
| 2020-03-12 08:48:05.485348 |          | 14087 COORDINATOR                      | 38-6e-21-ff-7e-12-80 | 111 | Robust        | 36 0x302d  | 128         |                   |                  |                       | 61 noise G3_FCC+DATA 0x0027 16 Bytes LBP (VasienGr)FFFF7A1280 ACCEPTED                |
| 2020-03-12 08:48:05.490201 |          | 4807                                   |                      | 116 | Robust        | 8          | 128         |                   |                  |                       | 21 noise G3_FCC ACK 0x0027  |
| 2020-03-12 08:48:05.515205 |          | 14551 0x0002                           | BROADCAST            | 116 | 206547 Robust | 38 0x302d  | 98          |                   |                  |                       | 63 noise G3_FCC+DATA 0x018c 18 Bytes Encrypted  |
| 2020-03-12 08:48:05.516776 |          | 14551 0x0002                           | BROADCAST            | 116 | Robust        | 38 0x302d  | 98          |                   |                  |                       | 63 noise G3_FCC+DATA 0x018c 18 Bytes Encrypted RREQ (n=2 encscb d=0)                  |

Figure 5- 17- Joining Process

## 5.2.5- Effects of Telegram Length

Another factor that plays an important role in the performance of the system, is the length of telegram. Different length of telegrams means different processing times and act as an decisive factor for calculation of reaction times.

As mentioned in 3.2.3.1.1, The number of symbols that need to be transmitted are entered in the FCH. In the Wireshark analyze we can see how many symbols every telegram has. Depending on the transmission method (Robust, DBPSK, DQPSK, D8PSK), the number of symbols determine the transmitted number of bytes of PSDU. This corresponds to the data length of the data field.

To calculate data rate, the number of symbols per PHY frame ( $N_s$ ), number of subcarriers per symbol ( $N_{CAR}$ ) and the number of parity bits added by FEC blocks are needed [10].

To calculate the data rate, table 5.4 showcases defined parameters for FCC band.

| Parameter              | Value   | Description  |
|------------------------|---------|--|
| CC <sub>Rate</sub>     | 1/2     | Rate for convolutional encoder   |
| CC <sub>Zerotail</sub> | 6 bits  | Added number of bits of convolutional encoder                              |
| N <sub>CAR</sub>       | 72      | Number of subcarriers per symbol in FCC Band from 154,687 kHz to 487,5 kHz |
| N                      | 256     | Number of FFT points   |
| N <sub>O</sub>         | 8       | Number of overlapped samples   |
| N <sub>CP</sub>        | 30      | Number of cyclic prefix samples  |
| N <sub>FCH</sub>       | 12      | Number of FCH symbols  |
| N <sub>pre</sub>       | 9,5     | Number of symbols in preamble  |
| f <sub>s</sub>         | 1,2 MHz | Sampling frequency   |

Table 5- 4- OFDM Modulator Control Parameters for FCC Band [15, P. 9 and 10. P. 9]

As the modulation modes explained in 3.2.3, in order to select the number of symbols in each PHY frame, two parameters are needed: the required data rate and the acceptable robustness. Reed-Solomon block sizes, repetition code and *mod\_size* (the number of bits per constellation symbol) for different modulation modes are summarized in table 5-5.

| Parameter                                 | Modulation                                     | Value   |
|---|--|---------|
| Repetition Code (Robust <sub>Rate</sub> ) | Robust   | 4       |
|   | DBPSK, BPSK, DQPSK, QPSK, D8PSK, 8-PSK, 16-QAM | 1       |
| Parity Byte (Reed_Solomon)                | Robust   | 8 Byte  |
|   | DBPSK, DQPSK, D8PSK                            | 16 Byte |
| Mod_size                                  | Robust, DBPSK, BPSK                            | 1       |
|   | DQPSK, QPSK                                    | 2       |
|   | D8PSK, 8-PSK                                   | 3       |
|   | 16-QAM   | 4       |

Table 5- 5- Modulation mode dependent parameters

During the smart grids test serie, different telegrams with different number of symbols and different modulation modes (8-PSK and mostly robust) are transferred and received. As an example the data rate and time of frame, transferring in in robust mode for telegrams with N<sub>S</sub>= 117, N<sub>S</sub>=128 and N<sub>S</sub>=130 (around 12800 from 16200 telegrams are with this size), with the help of 5-1, 5-2, 5-3 and 5-4 are calculated [10, P. 9].

$$\text{Total\_No\_Bits} = N_S \times N_{CAR} \quad (5-1)$$

$$\text{No\_Bits\_Robust} = \text{Total\_No\_Bits} \times \text{Robust}_{Rate} \quad (5-2)$$

The rate for convolutional encoder (CC<sub>Rate</sub>) is equal to ½ and to terminate the states of encoder to all zero states, 6 bits of zero is added (CC<sub>Zerotail</sub> = 6 bits). With 5-3, the maximum number of symbols at the output of the Reed-Solomon encoder (MAXRS<sub>Bytes</sub>) is calculated.

$$\text{MAXRS}_{Bytes} = \text{floor} \left( \frac{\text{No\_Bits\_Robust} \times \text{CC}_{Rate} - \text{CC}_{ZeroTail}}{8} \right) \quad (5-3)$$

8 bytes related to parity bits in robust mode is removed.

$$\text{DataLength}_{\text{bits}} = (\text{MAXRX}_{\text{Bytes}} - \text{ParityLength}) \times 8 \quad (5-4)$$

5-4 shows the data length that is carried in a duration of PHY frame. With 5-5, the duration of a PHY frame is calculated [10, Page 9]:

$$T_{\text{Frame}} = \frac{(N_S + N_{FCH}) \times (N_{CP} + N - N_O) + (N_{PRE} \times N)}{f_s} \quad (5-5)$$

Table 5-6 summarizes the calculations for different  $N_S$ .

| $N_S$ | DataLength (Bytes) | $T_{\text{Frame}}$ (mSec) | Data Rate (kbits/sec) |
|-------|--------------------|---------------------------|-----------------------|
| 117   | 122                | 31,91                     | 30,584                |
| 128   | 135                | 34,46                     | 31,340                |
| 130   | 137                | 34,92                     | 31,38                 |

Table 5- 6- Data Rate for different messages with different  $N_S$

As figure 5-18 showcases, if we see again the signal lifespan, the  $T_{\text{Frame}}$  calculated in table 5-6 shows the time the telegram message took.



Figure 5- 18-  $T_{\text{Frame}}$  in Signal Lifespan

## 5.2.6- Applicative Baud Rate

Apart from data rate of different telegrams calculated in 5.2.5, with the calculation of telegrams packet size through the whole time, that the network was busy, either for smart grids or for smart metering, a theoretical Applicative Baud Rate (*ApplBaudRate*) can be defined. But this Baud Rate is calculated for every smart meter separately. As Formula 5-6 showcases, the calculation is done through the sum of positive acknowledged telegrams divided by the time the network was busy for the data transmission of data packets. This means in this case, sum of the whole window time of data transmission between smart meters (25:23 in the smart metering test serie and 24:12 in the smart grids test serie).

$$ApplBaudRate = \frac{\text{Positive Acknowledged Telegrams Size}}{\text{Overall Time of Busied Network}} \quad 5-6$$

*ApplBaudRate* shows how much payload bits are transferred per time. Comparison of *ApplBaudRate* for different test series, gives us an overall view how the communication traffic because of jumping of telegrams of other devices during the  $\Delta SW_{rsp}$  (as discussed in 5.2.2) and also noises can affect the applicative waiting time for responding messages in G3-PLC. Table 5-7 showcases the *ApplBaudRate* for smart metering and smart grids test series respectively.

| Test Serie     | Smart Meter | <i>ApplBaudRate</i><br>(kBits/sec) |
|----------------|-------------|------------------------------------|
| Smart Metering | 0x0002      | 255,45                             |
|                | 0x0003      | 245,73                             |
|                | 0x0005      | 252,98                             |
| Smart Grids    | 0x0002      | 166,95                             |
|                | 0x0003      | 179,71                             |
|                | 0x0005      | 182,005                            |

Table 5- 7- *ApplBaudRate* for Smart Meters in Different Test Series

As table 5-7 showcases, the *ApplBaudRate* during the smart grids test serie significantly reduced. The main reasons, the traffic in telegrams for smart grid packets and also emerged noises in the network.

# 6

## Discussion

### 6.1- Experiences in Real PLC Networks

The G3-PLC protocol, especially the OFDM system model is designed for the data to be transmitted at very high speeds. In the FCC Band, it can reach a data rate of up to 300 kBit/s [10]. When we compare and analyze the messaging method of G3-PLC with AMIS CX1, as explained in chapter two, we can see that the network can behave in different ways as expected.

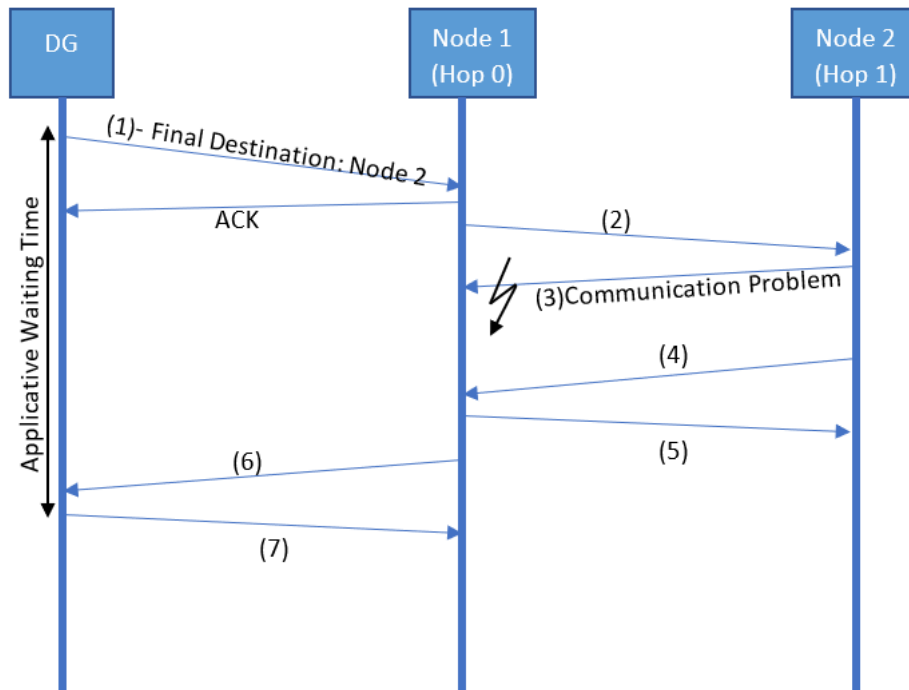


Figure 6- 1- Packet Flow in G3-PLC

As explained in 3.2.4, The messaging method in G3-PLC is developed in this way that if a data packet is missed on the way, the packet should be sent immediately again. As Figure 6-1 showcases, if a communication problem emerges (3), this packet cannot be received in node 1 and DG is not informed because the packet is lost on the way. When this occurs, the DG should wait for an applicative waiting time. The main problem with G3-PLC in big networks is the waiting time which is needed for the DG to get informed if the packet or the connection with the smart meter has been lost. This is because the DG cannot get updated on what is happening between these time periods.

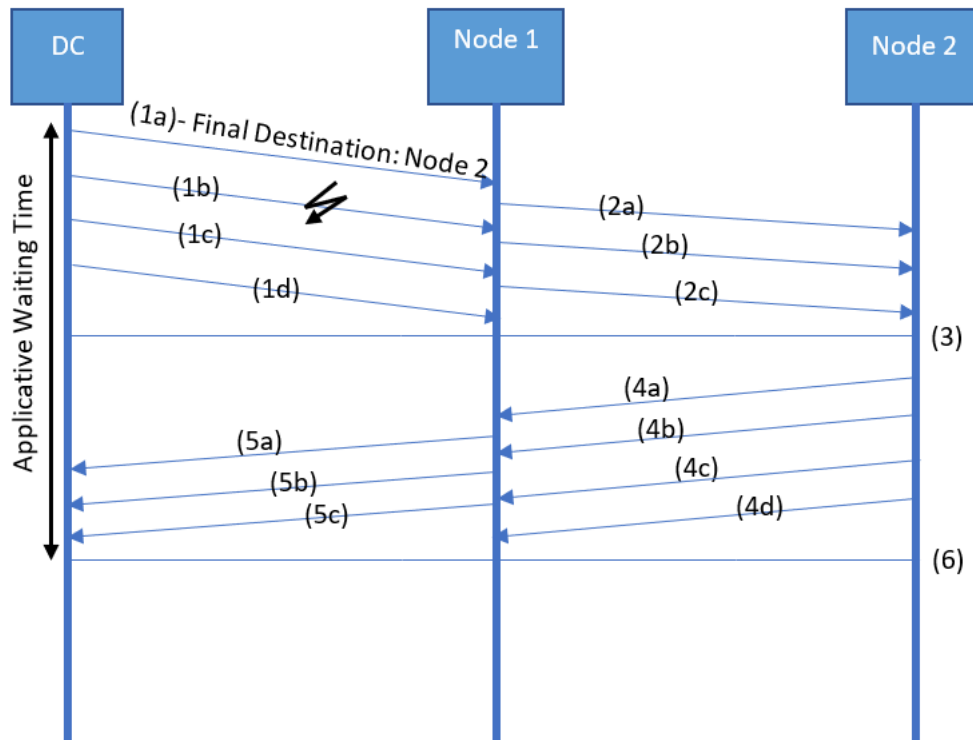


Figure 6- 2- Packet Flow in AMIS CX1

As explained in 2.5.2.1, in the AMIS CX1, the simultaneous forwarding of all the packets are sent in like a broadcast wave which is repeated in defined times with the help of a counter synchronously. The number of repeats of the packets, does not have anything to do with the number of hops (the number of meters in within DC and final destination node). This can also be seen in Figure 6-2. When DC wants to communicate with a node, it sends its packet as a broadcast message to all the nodes and repeats it up to eight times (number of repeats are definable) synchronously (1). After a node receives a packet, it waits for a specific short waiting time, until all the packets have arrived (3) and then responds with the same method. The final destination of the response packet (DC) will wait for a specific short waiting time even after receiving the response (6). The disadvantage for this messaging method is that the smart meters consume more energy in compare to smart meters in G3-PLC network, but instead the smart meters in AMIS CX1 does not have to perform and search for a route in network.

In a noise-free environment (unlike practical CENELEC-A band environment), data packets in G3-PLC can be sent and received significantly faster in compare to AMIS CX1. On the other hand, in a noisy environment, the mentioned applicative waiting time in G3-PLC (in a meshed network with more than 500 nodes per DG) can be much higher. This is because if there is any communication problem, DG should wait for a pre-defined time until it sends the data packet to the specified node again. This delay causes DG to misevaluate the situation (if there is no response in this time window), as it assumes it may have lost his connection with the smart meter and implements *Route\_Repair*. That causes even more delays. According to [19], “using RREQ floods whole network and in case of temporary bad conditions it can cause complete congestion of whole PAN (Personal Area Network)”. Due to this uncertainty from DG in G3-PLC, the applicative waiting time for DG is not calculable, unlike AMIS CX1, that knows exactly

how long sending a broadcast message can take and also knows the software processing times.

Apart from the data rate, another considerable factor is the packet lost rate. Packet lost rate shows in which percentage the data packets are lost. In a noisy environment the packet lost can be high. In AMIS CX1, if a communication problem emerges (Figure 5-20, (1b)), the node tries to repeat the packet, if still does not help, it repeats it more or changes the modulation method. The waiting time between every interval (because of its nature of calculable waiting time) becomes much shorter. In G3-PLC, if a communication problem emerges (Figure 5-19, (3)), the waiting time is longer, that causes in reduction of *ApplBaudRate*.

Regarding messaging method, the art of the system should also be studied. AMIS CX1 is a Master/Slave system. This has advantages and disadvantages. The disadvantage is when the smart meters have something to send, they are not allowed, they answer when they are asked. The advantage is the master (DC) takes the initiative and responsibility to allow who responds and who does not. For smart grids networks in AMIS CX1 with the help of time credit technique, the allocation of the maximum communication time (band width) for different AMIS functions are limited and definable [5]. In G3-PLC, as showcased in Figure 5-14, the emerging of data packets to/from other nodes between the communication of DG with another specific node, can cause delays in response and reduction of *ApplBaudRate* especially in big networks.

## 6.2- Conclusion

The G3-PLC technology is an international standard for data communication in electrical grids. High data rates as communication mediums in existing power infrastructures can be made possible which can be a thinkable option for smart grids solutions.

The G3-PLC technology uses the frequency band below 500 KHz for data communication [10], this allows for long distance data communication. In this project a method for implementing a smart grids network parallel with smart metering network is recommended. Through the labor tests in this thesis, a separate communication channel with the Modbus TCP/IP protocol is used.

It should also mentioned that, the research method (starting with AMIS CX1 project to study as a successful implementation of smart grids and smart metering parallel in a PLC network) and the proposed test system and analyze method used in this thesis, are tried to be seen from the point of view of a technician who are working in the real field, not as test engineers in labs or developers that conducts tests in a lab-environment. This brought me in this conclusion to criticize the G3-PLC protocol especially in **MAC layer**.

G3-PLC telecommunication technology has some specifications like mesh architecture, PSK modulation, OFDM, ensuring the fairness in media access through CSMA/CA mechanism, variable PHY packet length, PHY layer packet acknowledgement and LOADng routing protocol [19].

CSMA/CA access to media bring certain fairness to media access but setting the parameters for an optimal performance for different topologies of PAN network with different number of



nodes is impossible. This means that according to [19], “we always have to **have parameters prepared for worst case conditions**”.

G3-PLC communication method and its ROBO modulation technique bring us to the conclusion that it can be used in last-mile communication, mainly for solutions which response time is not critical (likw smart metering) [14]. This communication degraded by attenuation and noises. As explained in 5.2 and 5.3, considering **the importance of ApplBaudRate** in the analysis, G3-PLC protocol is designed to work in a medium where a proper communication is available, not in a very hostile environment like CENELEC-A band. This does not conclude that G3-PLC is not a proper solution. What should be mentioned is that only trying to improve the data rate (as proposed in G3-PLC protocol ITU G.990x), but not observing and considering the nature of hostile environment of CENELEC-A band and not taking account of *ApplBaudRate* in noisy channels makes us conclude that **G3-PLC is designed to work in a network with a very good communication environment**. Using filters can improve the status better. Also using the FCC band can be the best option for G3-PLC protocol (for its nature of noise-free environment), but as explained already because of EU regulations, currently there is no outlook in allocating FCC band for energy distributor companies.

As explained in 6.1, due to the nature of G3-PLC, which is not a Master/Slave system, any device can talk with DG. To overcome this problem, the solution can be, changing the node settings, e.g. how often they can communicate with the DG or changing parameters to allow or limits the media access through CSMA/CA method. But also, should be remembered that changing parameters to prepare for the worst-case scenario cannot always work efficiently in PLC networks. Considering the Master/Slave communication system for networks with smart metering and smart grids in parallel, relates also to organizational structure of energy distributor companies (in our case the client who uses the system). In energy distributor companies there are two different departments who are working with meter data. One is responsible for smart meters and uses consumption-data (pure smart metering data) and another department is responsible for smart grids and network quality improvement that uses smart grids data. This organizational structure brings us to the important reason for necessity of separate allocation of network usage from different departments and as a result separate allocation of dataflow in network used by different departments. **This can achieve only by a Master/Slave communication system, that is not fulfilled in G3-PLC protocol.**

The proposed method in this thesis, based on the results from chapter 5 is technically possible. Because of the defined main goal to see if actually a separate communication channel for smart grids data is possible, the test is conducted in FCC band (unlike the need for CENELEC band in real field). The second goal of this thesis to analyze the test results based on experiences in real field, to see how the reaction time changes with presence of smart grids data packets, made me to the conclusion that always trying to change parameters, using filters, implementing noise-clearing measures to improve the quality of network for a better communication cannot be an applicable option, **unless changes in messaging method and MAC layer of G3-PLC protocol** (as recommended in the last paragraphs and 6.1) are implemented from G3-PLC Alliance. AMIS CX1 is a good example of an already available communication solution for (smart grid) system automation [4]. However, due to its proprietary nature it has not been subject to a scientific discussion [4]. New PLC developments

often start from standardized and published solutions for wireless systems, such as IEEE 802.15-4. However, these solutions may not be a good fit for the power line channel and a lot of changes are necessary [4]. The result is not as good and efficient as it could be using a direct design approach, like how AMIS CX1 is designed and expected from G3-PLC Alliance to review back the available solutions in the market.

## 6.3- Outlook

Nowadays data communication among devices in an electrical grid can be done through PLC. Still some factors such as attenuation and noises of equipment can degrade the performance of the system [14]. Using the G3-PLC standard, carriers can be modulated using robust mode [10], a variation of BPSK modulation [14]. Also, in OFDM systems with robust mode, the FEC encoder consists of Reed-Solomon and convolutional encoders together with a repetition code. The repetition code repeats each bit four times [10], that according to [14], this is “making the system more robust to adverse conditions”. As Korki et al presented in [16] and is recommended for further tests in real field, the BER (Bit Error Rate) performance of the narrowband OFDM-Based PLC system is slightly improved by using the optimal Clipping/Blanking technique [16].

All the PLC solutions should fulfill the demands of Oesterreichs Energie (OE) use cases. Especially, the demanding SLA (Service Level Agreement) is a challenge. According to current European standard [17], use of CENELEC-A Band for energy distributor companies is compulsory. The communication in low voltage in CENELEC-A Band is based on experiences are very hostile and noisy and performance of PLC communication is “significantly degraded by the impulsive noise with very large amplitudes and short durations” [16]. To this end, an extension of this test results in CENELEC-A Band through a discussion with producers of measuring devices (Siemens, Devolo, etc.) is recommended.

# Literature

[1] AMIS Smart Grid Metering System Katalog AMIS V1.0- Online:

[https://www.quad-industry.com/titan\\_img/ecatalog/AMIS\\_Smart\\_Metering\\_System\\_de\\_LeseLinks.pdf](https://www.quad-industry.com/titan_img/ecatalog/AMIS_Smart_Metering_System_de_LeseLinks.pdf)

Downloaded on 17 Sep. 2020

[2] „Augen im Netz“: Neue Wege der Analyse elektrischer Niederspannungsnetze, A. Abart OVE, M. Stifter OVE, B. Bletterie, H. Brunner, D. Burnier, R. Pointner, A. Schenk, R. Pitz, H. Taus, 2011- Online:

<https://link.springer.com/article/10.1007/s00502-011-0821-y> – Downloaded on 17 Sep. 2020

[3] AMIS Smart Grid Funktionen- Benutzerhandbuch

[4] T.G. Lutz Lampe, Andrea M. Tonello, Power Line Communications: Principles, Standards and Applications from Multimedia to Smart Grid, 2<sup>nd</sup> ed. Wiley 2016

[5] SIEMENS, AMIS CX1-Profil (Compatibility/Consistently Extendable Transport Profile V.1) Layer 1-4. SIEMENS, 2011

[6] O. Energie, SMART Metering USE-Cases für das Advanced Meter Communication System (AMCS), v1.1 ed. Oesterreichs Energie, 2015- Online:

[https://oesterreichsenergie.at/files/Downloads%20Netze/Oesterreich%20Use%20Cases%20Smart%20Metering\\_14122015\\_Version\\_1-1.pdf](https://oesterreichsenergie.at/files/Downloads%20Netze/Oesterreich%20Use%20Cases%20Smart%20Metering_14122015_Version_1-1.pdf) – Downloaded on 17 Sep 2020

[7] Auswirkung der Paket Size auf das G3-Protokoll im CENELEC-A Band, Bachelor thesis by Ing. Kurt Hochleitner- 17 Mai. 2018

[8] MODBUS Messaging on TCP/IP Implementation Guide V1.0b , MODBUS Organization- Online:

[https://modbus.org/docs/Modbus\\_Messaging\\_Implementation\\_Guide\\_V1\\_0b.pdf](https://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf)

Downloaded on 17 Sep. 2020

[9] The Lightweight On-demand Ad hoc Distance-vector Routing Protocol – Next Generation (LOADng) draft-clausen-lln-loadng-15, Network Working Group, July 4, 2016- Online:

<https://tools.ietf.org/html/draft-clausen-lln-loadng-15> – Downloaded on 17 Sep. 2020

[10] ITU-T G.9903, Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks, (02/2014)- Online:

<https://www.itu.int/rec/T-REC-G.9903-201402-S/en> – Downloaded on 17 Sep. 2020

[11] SIEMENS, AMIS CX1-Profil (Layer 2-4) DLC Kommunikationsprotokoll Gemeinschaftsverkehr (Master/Slave) , 2014

[12] Power Monitoring Device SENTRON PAC3200- Manual. Online:

[https://cache.industry.siemens.com/dl/files/150/26504150/att\\_906558/v1/A5E01168664B-04\\_EN-US\\_122016\\_201612221316360495.pdf](https://cache.industry.siemens.com/dl/files/150/26504150/att_906558/v1/A5E01168664B-04_EN-US_122016_201612221316360495.pdf)

Downloaded on 16 Sep. 2020

[13] Enhanced 6LoWPAN Ad Hoc Routing for G3-PLC, K. Razazian, A. Niktash, V. Loginov, J. Yazdani, Online:

<https://ieeexplore.ieee.org/abstract/document/6525839/authors#authors>

Downloaded on 17 Sep. 2020

[14] Empirical Analysis of the Communication in Industrial Environment Based on G3-Power Line Communication and Influences from Electrical Grid, Luiz da Rocha Farias, Lucas Felipe Monteiro, Murilo Oliveira Leme and Sergio Luiz Stevan Jr., Published: 11 September 2018 – Online:

[https://www.researchgate.net/publication/327585925\\_Empirical\\_Analysis\\_of\\_the\\_Communication\\_in\\_Industrial\\_Environment\\_Based\\_on\\_G3-](https://www.researchgate.net/publication/327585925_Empirical_Analysis_of_the_Communication_in_Industrial_Environment_Based_on_G3-Power_Line_Communication_and_Influences_from_Electrical_Grid)

[Power Line Communication and Influences from Electrical Grid](https://www.researchgate.net/publication/327585925_Empirical_Analysis_of_the_Communication_in_Industrial_Environment_Based_on_G3-Power_Line_Communication_and_Influences_from_Electrical_Grid)

Downloaded on 17 Sep. 2020

[15] ITU-T G.9901, Narrowband orthogonal frequency division multiplexing power line communication transceivers- Power spectral density specification, (06/2017)- Online:

<https://www.itu.int/rec/T-REC-G.9901-201706-I/en> – Downloaded on 17 Sep. 2020

[16] Performance Evaluation of a Narrowband Power Line Communication for Smart Grid with Noise Reduction Technique. Mehdi Korki, Nasser Hosseinzadeh, Senior Member, IEEE, and Taleb Moazzeni, IEEE Transactions on Consumer Electronics, Vol. 57, No. 4, November 2011 Online:

[https://www.researchgate.net/publication/239766457\\_Performance\\_evaluation\\_of\\_a\\_narrowband\\_power\\_line\\_communications\\_for\\_Smart\\_Grid\\_with\\_noise\\_reduction\\_technique](https://www.researchgate.net/publication/239766457_Performance_evaluation_of_a_narrowband_power_line_communications_for_Smart_Grid_with_noise_reduction_technique)

Downloaded on 17 Sep. 2020

[17] EU Mandat 441/EN- Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability.

Online: <http://www.etsi.org/images/files/ECMandates/m441%20EN.pdf>

Downloaded on 17 Sep. 2020

[18] G3-PLC User Guidelines, Introduction of G3-PLC for non-experts (Version 1.0, 04/2020)- Online:

[http://www.g3-plc.com/fileadmin/user\\_upload/What\\_is\\_G3PLC/G3-PLC Alliance PLC introduction for non experts 1.0 PUB April2020.pdf](http://www.g3-plc.com/fileadmin/user_upload/What_is_G3PLC/G3-PLC_Alliance_PLC_introduction_for_non_experts_1.0_PUB_April2020.pdf)

Downloaded on 17 Sep. 2020

[19] Performance analysis among s\_FSK, G3-PLC V2015 and G3-PLC V2017, Jure Germovsek, Janez Zavasnik- Online:

<http://wsplc2018.fe.uni-lj.si/wp-content/uploads/2018/09/P2-Iskraemeco-F.pdf>

Downloaded on 17 Sep. 2020

[20] DG DemoNet- Smart LV Grid. Online:

<https://www.energieforschung.at/assets/project/downloads/DG-Demonet-Smart-Grid-Erkenntnisse-fuer-die-Integration-dezentraler-Erzeugung.pdf> , downloaded on 14 Sep. 2020

[21] Benchmarking smart metering deployment in the EU-28, Final Report- European Commission. Online:

<https://op.europa.eu/en/publication-detail/-/publication/b397ef73-698f-11ea-b735-01aa75ed71a1/language->

[en?WT.mc\\_id=Searchresult&WT.ria\\_c=37085&WT.ria\\_f=3608&WT.ria\\_ev=search](https://op.europa.eu/en?WT.mc_id=Searchresult&WT.ria_c=37085&WT.ria_f=3608&WT.ria_ev=search)

downloaded on 14 Sep. 2020

[22] IEEE 802.15.4-2020 IEEE Standard for Low-Rate Wireless Networks- Online:

<https://ieeexplore.ieee.org/document/7460875> - downloaded on 14 Sep. 2020

[23] DLMS User Association- DLMS/Cosem Architecture and Protocols (Green Book- Edition 8,3), 2017. Online: <https://www.dlms.com/files/Green-Book-Ed-83-Excerpt.pdf>

downloaded on 16 Sep. 2020

[24] Modbus and ION Technology, Technical Note published by Schneider Electric, 2009.

Online: <https://download.schneider->

[electric.com/files?p\\_enDocType=User+guide&p\\_File\\_Name=70072-0104-](https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=70072-0104-14.pdf&p_Doc_Ref=70072-0104-14)

[14.pdf&p\\_Doc\\_Ref=70072-0104-14](https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=70072-0104-14.pdf&p_Doc_Ref=70072-0104-14) - Downloaded on 16 Sep. 2020

[25] Smart Metering. Online:

<https://www.wienerstadtwerke.at/eportal3/ep/programView.do/pageTypeId/71282/programId/73088/channelId/-51344> -Downloaded on 23 Oct. 2020

# List of Figures

|       |   |    |
|-------|---|----|
| 2-1-  | AMIS Configuration Overview   | 7  |
| 2-2-  | AMIS Communication Model  | 8  |
| 2-3-  | Principle of Phase Grouping   | 9  |
| 2-4-  | Voltage characteristics along the line in classical LV Network                    | 10 |
| 2-5-  | Packet structure of the physical layer of AMIS CX1                                | 12 |
| 2-6-  | Signals in basic transmission mode of AMIS CX1                                    | 13 |
| 2-7-  | Illustration of Simultaneous Forwarding from Master to destination Slave (-->)    | 15 |
| 2-8-  | Illustration of Response From Slave to Master in a Simultaneous Forwarding System | 16 |
| 3-1-  | OSI reference model of ITU-T G.9903 G3-PLC standard                               | 19 |
| 3-2-  | ITU-T G.9903 G3-PLC PHY layer transmitter   | 20 |
| 3-3-  | Data Frame Structure of a G3-Frame  | 22 |
| 3-4-  | FCH Structure   | 23 |
| 3-5-  | MAC-Header Structure  | 23 |
| 3-6-  | Example of neighbor and routing tables for ITU-T G.9903 G3-PLC MAC layer          | 24 |
| 3-7-  | Flowchart explaining the directional link cost computation                        | 27 |
| 4-1-  | Noise Scenario on Power Line  | 31 |
| 4-2-  | Infrastructure Symbol   | 32 |
| 4-3-  | System Architecture of G3-Solution for Smart Metering                             | 32 |
| 4-4-  | Gateway Protocol Header   | 33 |
| 4-5-  | DLMS request from HES to End-Device with Gateway Protocol                         | 33 |
| 4-6-  | DLMS COSEM UDP  | 34 |
| 4-7-  | Integration of G3-Protocol in DLMS Architecture                                   | 35 |
| 4-8-  | Integration of G3-Protocol in OSI Model   | 35 |
| 4-9-  | OSI Model for TCP/IP Ethernet Data Packet   | 38 |
| 4-10- | Client-Server Messaging Model   | 39 |
| 4-11- | General Modbus Frame  | 39 |
| 4-12- | Modbus Request/Response over TCP/IP   | 39 |

|       |  |    |
|-------|--|----|
| 5-1-  | Real Test System Structure- (a): Smart Meter Side, (b): Data Gateway Side  | 41 |
| 5-2-  | Test System Schematic Structure  | 41 |
| 5-3-  | DG-Application User Interface  | 42 |
| 5-4-  | Joined Devices on DG   | 42 |
| 5-5-  | Data Points (Modbus Holding Registers) defined for DG  | 43 |
| 5-6-  | Data Points (Modbus Holding Registers) defined for Modbus Simulator  | 43 |
| 5-7-  | Transferred Values from Modbus Simulator to DG   | 44 |
| 5-8-  | Spontaneous Read-Out of meter data through UDIS HES  | 44 |
| 5-9-  | Wireshark Files nBox   | 44 |
| 5-10- | AES Key for nBox   | 45 |
| 5-11- | Outline of Telegram Packet in (a) Wireshark and (b) DG-Application   | 45 |
| 5-12- | Time calculation in DG-Application   | 46 |
| 5-13- | Signal Lifespan  | 48 |
| 5-14- | Communication of other devices during $\Delta SW_{rsp}$  | 48 |
| 5-15- | Effects of Noises in the Overall Performance   | 49 |
| 5-16- | Average $rspDelta$ in every minute in the Smart Grids Test Serie<br>(a) real (b) in the absence of background noises | 49 |
| 5-17- | Joining Process  | 50 |
| 5-18- | $T_{Frame}$ in Signal Lifespan   | 52 |
| 6-1-  | Packet Flow in G3-PLC  | 54 |
| 6-2-  | Packet Flow in AMIS CX1  | 55 |



# List of Tables

|      |   |    |
|------|---|----|
| 1-1- | PLC network requirements list for a PLC testbed in Germany                                    | 3  |
| 2-1- | Class distribution of voltage bands   | 10 |
| 3-1- | Major technical features of the ITU-T G.9903 G3-PLC standard                                  | 19 |
| 3-2- | Different Frequency Bands Supported by ITU-T G.9903 G3-PLC standard                           | 20 |
| 3-3- | Maximum data rates of ITU-T G.9903 G3-PLC standard at PHY layer                               | 21 |
| 3-4- | Parameters for FCH Structure  | 23 |
| 4-1- | MBAP Header fields description  | 39 |
| 4-2- | Areas of Modbus Interface   | 40 |
| 5-1- | Analyze of reaction time based on the telgerams arrived in DG-Application                     | 47 |
| 5-2- | Analyze of reaction times of smart metering test serie based on the telgerams arrived in nBox | 47 |
| 5-3- | Analyze of reaction times of smart grids test serie based on the telgerams arrived in nBox    | 47 |
| 5-4- | OFDM Modulator Control Parameters for FCC Band  | 51 |
| 5-5- | Modulation mode dependent parameters  | 51 |
| 5-6- | Data Rate for different messages with different $N_s$   | 52 |
| 5-7- | <i>ApplBaudRate</i> for Smart Meters in Different Test Series                                 | 53 |

# List of Acronyms

|                     |  |
|---------------------|--|
| <b>6LoWPAN</b>      | IPv6 over Low-Power Wireless Personal Area Network           |
| <b>ACK</b>          | Acknowledgement  |
| <b>ADU</b>          | Application Data Unit  |
| <b>AES</b>          | Advanced Encryption Standard                                 |
| <b>AM</b>           | Amplitude Modulation   |
| <b>AMCS</b>         | Advanced Metering Communication System                       |
| <b>AMIS</b>         | Automated Metering and Information System                    |
| <b>AMIS-DC</b>      | AMIS Data Concentrator                                       |
| <b>APDU</b>         | Application Protocol Data Unit                               |
| <b>ApplBaudRate</b> | Applicative Baud Rate  |
| <b>ARIB</b>         | Association of Radio Industries and Businesses               |
| <b>BB</b>           | Broadband  |
| <b>BPL</b>          | Broadband over Power Line                                    |
| <b>BPSK</b>         | Binary Phase-shift Keying                                    |
| <b>CCM</b>          | Cypher Counter Mode  |
| <b>CENELEC</b>      | Comité Européenne de Normalisation Electrotechnique          |
| <b>CSMA</b>         | Carrier Sense Multiple Access                                |
| <b>CSMA/CA</b>      | Carrier Sense Multiple Access with Collision Avoidance       |
| <b>CX1 Profile</b>  | Compatibly/Consistently Extendable Transport Profile V.1     |
| <b>D8PSK</b>        | Differential 8-Phase Shift Keying                            |
| <b>DBPSK</b>        | Binary DPSK  |
| <b>DC</b>           | Data Concentrator  |
| <b>DG</b>           | Data Gateway   |
| <b>DLC</b>          | Distribution Line Carrier                                    |
| <b>DLL</b>          | Data Link Layer  |
| <b>DLMS</b>         | Device Language Message Specification                        |
| <b>DPSK</b>         | Differential Phase Shift Keying                              |
| <b>DQPSK</b>        | Quaternary DPSK (Differential Quadrature Phase Shift Keying) |
| <b>DR</b>           | Demand Response  |
| <b>DSL</b>          | Digital Subscriber Line                                      |
| <b>DSM</b>          | Demand Side Management                                       |
| <b>ERDF</b>         | Electricité Réseau Distribution France                       |
| <b>EUI</b>          | Extended Unique Identifier                                   |
| <b>FCC</b>          | Federal Communications Commission                            |
| <b>FCH</b>          | Frame Control Header   |
| <b>FEC</b>          | Forward Error Correction                                     |
| <b>FFT</b>          | Fast Fourier Transform                                       |
| <b>FO</b>           | Fiber Optics   |
| <b>HDR</b>          | High Data Rate   |
| <b>HES</b>          | Head End System  |
| <b>HV</b>           | High Voltage   |
| <b>ICMP</b>         | Internet Control Message Protocol                            |
| <b>ICT</b>          | Information and Communication Technology                     |
| <b>IEC</b>          | International Electrotechnical Commission                    |
| <b>IEEE</b>         | Institute of Electrical and Electronics Engineers            |

|              |  |
|--------------|--|
| <b>IEFT</b>  | Internet Engineering Task Force            |
| <b>IFFT</b>  | Inverse Fast Fourier Transform             |
| <b>IP</b>    | Internet Protocol                          |
| <b>ITU</b>   | International Telecommunication Union      |
| <b>KMS</b>   | Key Management System                      |
| <b>LAN</b>   | Local Area Network                         |
| <b>LDR</b>   | Low Data Rate                              |
| <b>LQI</b>   | Link Quality Indicator                     |
| <b>LSF</b>   | Last Segment Flag                          |
| <b>LV</b>    | Low Voltage                                |
| <b>LW</b>    | Long Wave                                  |
| <b>MAC</b>   | Medium Access Control                      |
| <b>MBAP</b>  | MODBUS Application Protocol                |
| <b>MOD</b>   | Modulation                                 |
| <b>MTU</b>   | Maximum Transmission Unit                  |
| <b>MV</b>    | Medium Voltage                             |
| <b>NB</b>    | Narrowband                                 |
| <b>nBox</b>  | Neuron Box                                 |
| <b>OE</b>    | Oesterreichs Energie                       |
| <b>OFDM</b>  | Orthogonal Frequency-Division Multiplexing |
| <b>OSI</b>   | Open System Interconnection                |
| <b>PDC</b>   | Phase Detection Counter                    |
| <b>PDU</b>   | Protocol Data Unit                         |
| <b>PHY</b>   | Physical                                   |
| <b>PLC</b>   | Power Line Communication                   |
| <b>PSC</b>   | Power Supply Company                       |
| <b>PSDU</b>  | PHY Service Data Unit                      |
| <b>PSK</b>   | Phase Shift Keying                         |
| <b>PSS</b>   | Power Snap-Shot                            |
| <b>PSSA</b>  | Power Snap-Shot Analysis                   |
| <b>PV</b>    | Photovoltaic                               |
| <b>QAM</b>   | Quadrature Amplitude Modulation            |
| <b>RC</b>    | Route Cost                                 |
| <b>ROBO</b>  | Robust Modulation                          |
| <b>RREQ</b>  | Route Request                              |
| <b>RREP</b>  | Route Reply                                |
| <b>RS</b>    | Reed-Solomon                               |
| <b>SCADA</b> | Supervisory Control And Data Acquisition   |
| <b>SFN</b>   | Single Frequency Network                   |
| <b>SLA</b>   | Service Level Agreement                    |
| <b>SLF</b>   | Super Low Frequency                        |
| <b>SNR</b>   | Signal-to-noise Ratio                      |
| <b>TCP</b>   | Transmission Control Protocol              |
| <b>UDP</b>   | User Datagram Protocol                     |
| <b>ULF</b>   | Ultra Low Frequency                        |
| <b>UNB</b>   | Ultra-Narrowband                           |
| <b>WAN</b>   | Wide Area Network                          |
| <b>WL</b>    | Weak Link                                  |



TECHNISCHE  
UNIVERSITÄT  
WIEN

Ich habe zur Kenntnis genommen, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

## Diplomarbeit

Hiermit erkläre ich, dass die vorliegende Arbeit „Mögliche Lösungen für die Trafostationsautomatisierung in einem G3-PLC Netzwerk“ ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel, angefertigt wurde. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet.

Die Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder in ähnlicher Form in anderen Prüfungsverfahren vorgelegt.

Wien, im November 2020

---

Behzad Parvin