Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

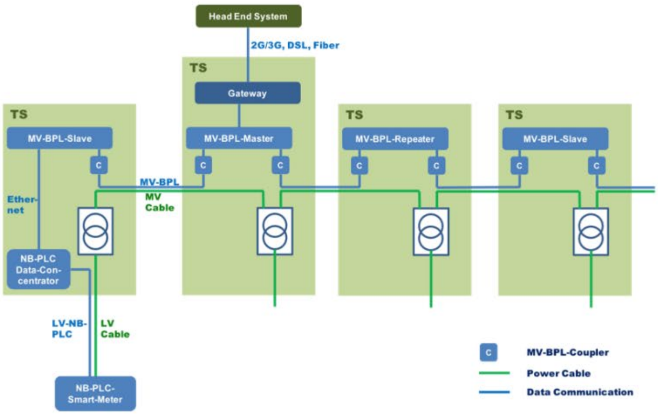
Department of the Environment,
Transport, Energy and Communication DETEC

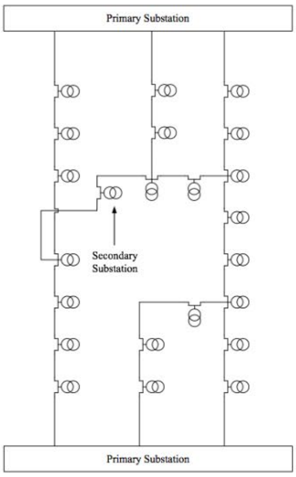
Swiss Federal Office of Energy SFOE
Energy Research

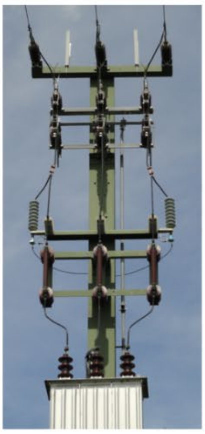
Final report 30.01.2019

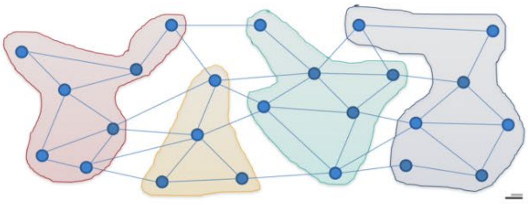
Mission- & Time-Critical Medium Voltage Broadband Power Line Communications for Synchrophasor Applications in the Distribution Grid

MV-BPL
for
Mission- and Time-Critical
Applications









Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Engineering and Architecture
FH Zentralschweiz

Date: 30 January 2019

Place: Horw

Publisher:
Swiss Federal Office of Energy SFOE
Research Programme Grids
CH-3003 Bern
www.bfe.admin.ch
energieforschung@bfe.admin.ch

Agent:
Lucerne University of Applied Sciences and Arts (HSLU)
Technikumstrasse 21, CH-6048 Horw
www.hslu.ch

Author:
Stephen Dominiak, Lucerne University of Applied Sciences and Arts, stephen.dominiak@hslu.ch
Ulrich Dersch, Lucerne University of Applied Sciences and Arts, ulrich.dersch@hslu.ch

SFOE head of domain: Dr Michael Moser, michael.moser@bfe.admin.ch
SFOE programme manager: Dr Michael Moser, michael.moser@bfe.admin.ch
SFOE contract number: SI/501504-01

The author of this report bears the entire responsibility for the content and for the conclusions drawn therefrom.

Summary

Worldwide, increasing pressure is being placed on the electric grids and, in particular, the Medium Voltage (MV) grids due to the increasing introduction of Distributed Energy Resources (DER). Grids must be able to accommodate new energy flow patterns in a more dynamic environment. This leads to the need not only for increasing the monitoring of the grid, but also to actively detect and mitigate the influence of potential faults in the grid. This requires Mission-and-Time-Critical (MTC) applications such as Phasor Measurement Units (PMU) measuring synchrophasors or Line Differential Protection (LDP). However, the communication requirements of such applications (high availability, low latency) provide a significant challenge to the communication infrastructure.

The motivation behind this project has been the development of a new Grid Monitoring & Automation (GMA) solution which takes advantage of the full potential of Broadband Power Line Communications (BPL) for enabling GMA applications in the MV grid. The major advantage provided by a MV-BPL solution is the low-cost communications infrastructure as the MV grid serves also as the communications medium. This goal has been achieved by adapting the MV-BPL technology in order to enable MTC functionality including time synchronization, higher availability and low-latency. Optimizations to the MV-BPL protocol have been aided through a model-based design approach in a simulation environment. The optimizations have been realized on a series of prototypes and tested within a laboratory environment as well as on a MV overhead test line at HSLU. Testing has shown that the developed MTC-MV-BPL solution can meet the strict requirements of LDP and PMU applications. Further field trials with the MTC-MV-BPL technology will now be performed in a follow-up “Pilot and Demo” project partially funded by SFOE.

Résumé

De manière globale, une pression grandissante est appliquée sur les réseaux électriques, et en particulier sur les réseaux de moyennes tensions (MT). La cause étant l’introduction croissante des ressources énergétiques distribuées (RED). Ainsi, les réseaux doivent être capables de s’adapter à de nouveaux modèles de flux d’énergie dans un environnement plus dynamique. Il est donc nécessaire d’augmenter la surveillance du réseau ainsi que d’activement détecter et réduire l’influence de potentielles erreurs dans les réseaux électriques. Ces genres de contrôles requièrent des applications telles que des unités de mesure de phaseurs (Phasor Measurement Unit - PMU) qui permettent, entre autres, la protection différentielle de lignes. De façon générale, les exigences de telles applications, grande disponibilité et courte latence, induisent un grand défi pour les infrastructures de communication.

La motivation derrière ce projet a été le développement d’une nouvelle solution pour la surveillance et l’automatisation des réseaux électriques, basée sur les avantages de la communication par courant porteurs en ligne (Broadband Power Line Communication - BPL) qui permettent l’intégration d’applications de surveillance et d’automatisation dans les réseaux MT. L’avantage majeur de la technologie BPL, utilisée dans les réseaux de moyennes tensions (BPL-MT), est le bas coût des infrastructures de communication, le réseau électrique existant servant également de moyen de communication. L’objectif a été atteint en adaptant la technologie BPL-MT, en activant les fonctionnalitées MTC (Mission-and-Time-Critical) lequelles incluent la synchronisation d’horloge, une disponibilité accrue ainsi qu’une latence réduite. Les optimisations apportées au protocole BPL-MT ont été réalisées, dans un premier temps, à l’aide d’une approche conceptuelle basée sur un model exécuté dans un environement de simulation. Par la suite, des prototypes ont été élaborés, puis testés en laboratoire ainsi que sur une ligne de test MT à l’HLSU. Les tests ont montré que la solution développée, BPL-MT-MTC, couvre les exigences requises pour la protection différentielle de lignes et des applications utilisant des PMU. De plus amples essais utilisant cette technologie, BPL-MT-MTC, seront effectués lors du prochain projet, pilote et de démonstration, partiellement fondé par SFOE.

Zusammenfassung

Weltweit wird durch die zunehmende Einführung von dezentralen Energiequellen ein wachsender Druck auf die elektrischen Netze und insbesondere auf die Mittelspannungsnetze (MS-Netz) ausgeübt. Die Netze müssen in der Lage sein, neue Energieflussmuster in einem dynamischen Umfeld aufzunehmen. Daraus ergibt sich die Notwendigkeit, nicht nur die Überwachung des Netzes zu erhöhen, sondern auch den Einfluss potenzieller Störungen im Netz aktiv zu erkennen und zu minimieren. Dies erfordert Mission- und Time-Critical (MTC) Anwendungen wie Phasor Measurement Units (PMU), die Synchrophasoren messen, oder Line Differential Protection (LDP). Die Kommunikationsanforderungen solcher Anwendungen (hohe Verfügbarkeit, geringe Latenzzeiten) stellen jedoch eine grosse Herausforderung für die Kommunikationsinfrastruktur dar.

Die Motivation für dieses Projekt war die Entwicklung einer neuen Grid Monitoring & Automation (GMA) -Lösung, die das volle Potenzial der Broadband Power Line Communications (BPL) für GMA-Anwendungen im MS-Netz nutzt. Der grosse Vorteil einer MS-BPL-Lösung ist die kostengünstige Kommunikationsinfrastruktur, da das MS-Netz selbst als Kommunikationsmedium dient. Dieses Ziel wurde durch Anpassungen der MS-BPL-Technologie erreicht, welche MTC-Funktionen wie Zeitsynchronisation, hohe Verfügbarkeit und niedrige Latenzzeiten ermöglichen. Optimierungen des MS-BPL-Protokolls wurden in einer Simulationsumgebung durch den Model-Based Design Ansatz realisiert. Die Umsetzung erfolgte anhand mehrerer Prototypen, welche in Laborumgebung sowie auf einer MS-Freileitung an der HSLU getestet wurden. Die Tests haben gezeigt, dass die entwickelte MTC-MS-BPL-Lösung die hohen Anforderungen von LDP- und PMU-Anwendungen erfüllen kann. Weitere Feldversuche mit der MTC-MS-BPL-Technologie werden nun in einem vom BFE mitfinanzierten Pilot- und Demonstrationsprojekt durchgeführt.

Contents

List of abbreviations

AC	Alternating Current
ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
AFE	Analog Front End
AMI	Automated Metering Infrastructure
ARP	Address Resolution Protocol
ARQ	Automated Repeat Request
ASIC	Application-Specific Integrated Circuit
AWGN	Additive White Gaussian Noise
BDS	Beacon Data Service
BER	Bit Error Rate
BKW	Bernische Kraftwerke AG
BPL	Broadband Power Line Communications
BPSK	Binary Phase-Shift Keying
BRAM	Block-RAM
CBC	Cipher Block Chaining
CF	Classical Flooding
CFP	Contention Free Period
CP	Contention Period
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CSMA/CP	Carrier Sense Multiple Access / Collision Prevention
CTC	Convolutional Turbo Code
DAC	Digital-to-Analog Converter
DAG	Design Assurance Guidelines
DAK	Device Access Key
DC	Direct Current
DER	Distributed Energy Resources
DFT	Discrete Fourier Transform
DLL	Data Link Layer
DNO	Distribution Network Operator
DPD	Duplicate Packet Detection
DS	Data Service

DSP	Digital Signal Processing
EAP	Extensible Authentication Protocol
EDS	Ethernet Data Service
EMC	Electromagnetic Compatibility
FC	Frame Control
FDM	Frequency Division Multiplexing
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FO	Fiber Optic
FOCA	Swiss Federal Office of Civil Aviation
FPGA	Field Programmable Gate Array
GB	Gateway Bridge
GMA	Grid Monitoring and Automation
GPS	Global Positioning System
HD	Hamming Distance
HIL	Hardware-in-the-Loop
HIRF	High Intensity Radiated Fields
HSLU	Lucerne University of Applied Sciences and Arts
HW	Hardware
IFFT	Inverse Fast Fourier Transform
IFS	Inter-Frame Spacing
ILA	Integrated Logic Analyzer
IP	Internet Protocol
LAN	Local Area Network
LDP	Line Differential Protection
LLC	Logical Link Control
LNA	Low Noise Amplifier
LUT	Lookup-Table
LV	Low Voltage
MAC	Medium Access Control
MBD	Model Based Design
MCS	Modulation and Coding Scheme
MPDU	MAC protocol data unit
MSDU	MAC Service Data Unit
MTC	Mission- and Time-Critical
MV	Medium Voltage
NMEA	National Marine Electronics Association

NMK	Network Management Key
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection (Model)
PB	Physical Blocks
PCF	Point Coordination Function
PCS	Protection Communication Service
PDN	Power Distribution Network
PHY	Physical Layer
PL	Programmable Logic
PLC	Power Line Communication
PLS	Physical Layer Security
PLUS	Power Line data bUS
PMU	Phasor Measurement Unit
PPDU	PHY Protocol Data Unit
PPS	Pulse Per Second
PS	Primary Substation
PS	Processing System
PSD	Power Spectral Density
PUD	Probability of occurrence of Undetected errors
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase-Shift Keying
R2MDC	Radix-2 Multi-path Delay Commutator
RAM	Random-Access Memory
SFOE	Swiss Federal Office of Energy
SISO	Soft Input / Soft Output
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SoC	System-on-Chip
SQNR	Signal-to-Quantization-Noise Ratio
SS	Secondary Substation
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TEK	Temporary Encryption Key
TRL	Technology Readiness Level
UKE	Unicast Key Exchange
V&V	Verification and Validation
VGA	Variable Gain Amplifier

VHDL	Very High Speed Integrated Circuit Hardware Description Language
WAN	Wide Area Network

1 Introduction

1.1 Overview

Worldwide, increasing pressure is being placed on the electric grids and in particular the Medium Voltage (MV) grids due to the steadily increasing introduction of Distributed Energy Resources (DER). The highly time-dynamic character of such power fed into the grid by a vast amount of spatially distributed sources combined with the decreasing ratio of stabilizing rotational mass leads to substantial challenges for the future grids to keep them robust enough for the requirements and expectations of the consumers. Grids must be able to accommodate new energy flow patterns in a considerably more dynamic environment.

Therefore, protection and automation systems are quickly gaining importance not only for the transmission grid but increasingly at the distribution grid level for the asset management programs of Distribution Network Operators (DNOs). This leads to the need not only for increasing the monitoring of the grid, but also to actively detect and mitigate the influence of potential faults in the grid. This requires critical applications such as voltage/congestion control and fault detection/location.

Phasor Measurement Units (PMU) measuring synchrophasors and Line Differential Protection (LDP) provide examples of such critical applications. They offer promising approaches for such high precision grid monitoring and automation. However, the communication requirements of such applications (high availability, low latency) provide a significant challenge to the communication infrastructure. Currently, there is no clear vision in the market on the exact communication technologies and network topologies which could fulfill these requirements. In any case there is a risk that such applications – which are well installed in the transmission grid today - in the distribution grid might lead to unacceptable cost figures which might prevent or in the best case delay the acceptance of such applications by DNO customers.

Such applications call for a larger amount of control and automation technology, but requiring at the same time cost-effectiveness in order to be bearable for the customers. For example, due to the pressure induced by the highly dynamic generation of renewables, it is no longer enough to use local measurements (V, I phasors and P,Q values) within each Secondary Substation (SS) for automation and protection, but more advanced monitoring and protection applications which require the exchange of measurements data between SSs are required. Distributed measurements between SSs will also be adding value by allowing the application of synchrophasors to the distribution level, helping to achieve efficient control of bidirectional power flows due to the massive integration of renewable energy systems.

These types of functionalities present a real challenge as the complete chain is involved, from the sensors, protection relays and various electronic devices integrated in the SS cubicle to the communication infrastructure to exchange the data between the SSs. Such communication infrastructure has to fulfil very high requirements regarding availability and latency, as will be described later on, and can therefore be considered as a Mission- and Time-Critical (MTC) communications infrastructure.

Considering the state-of-the-art in the communication infrastructure, there has already been a substantial change, as not long ago the communication equipment installed in these installations communicated through serial protocols with dispatch centers, due to the fact that the communication requirements were not very high in the electrical sector. However, still today there are only very few rollouts in which communications between SSs is provided.

Due to the large amount of SSs installed at the distribution level (ca. 4 Mio in Europe), the cost effectiveness of such applications including the communications system plays a critical role. Whereas Primary Substations (PS) at the transmission level are typically in an order of tens or few hundred, SSs are in an order of thousands or even tens of thousands for large utilities. A typical rule-of-thumb for DNOs is that the cost of equipment protecting the infrastructure should be less than 10% of the cost of the infrastructure to be protected. This further motivates a cost reduction of the protection equipment at the distribution level compared to the transport level.

Today’s communication technologies do not completely fulfil the communication requirements for the above described applications with costs which are tolerable for a wide deployment in the distribution grid:

- Cellular networks (2G/3G/4G): latency too high, availability dependent upon the network operator and on the network load of other users
- Fiber Optic (FO) networks: fulfils the communication requirements but a full FO infrastructure is not bearable due to its significantly high costs
- MV Broadband Power Line Communications (MV-BPL): today’s commercial technology does not support the reliability and latency requirements.

New solutions for the communication are therefore required, for fulfilling both the functional and the cost requirements.

1.2 Medium Voltage Broadband Power Line Communications

In this chapter an overview of the specific characteristics of a MV-BPL network will be provided which is partially necessary in order to understand the time-synchronization concepts presented later in this document. The MV distribution grid (i.e. 1 - 36 kV) comprises mainly underground cables, overhead lines and related infrastructure, including SSs. The MV grid mainly differs from the Low Voltage (LV) access and indoor grid in terms of the physical topology, cable/wire types and link distances. A broad range of SSs can be found depending upon the area (urban, suburban or rural) and consumption levels. Big utilities may operate hundreds of thousands of SSs. Such a heterogeneous set of SSs, however, presents a fundamental common infrastructure: MV lines which interconnect SSs among themselves and to PSs. The underlying topology of this interconnection can be considered as a meshed ring topology in which a certain amount of redundancy is provided between SSs and PSs. Links between SSs are usually very heterogeneous with several different cable types as well as a combination of overhead lines and underground cables being found in a single geographical area. While underground cables represent point-to-point links with relatively stable loads and impedances, overhead MV lines, on the contrary, may present taps in a tree-like topology.

One typical misconception regarding the use of BPL in MV grids is that link distances are too long to support any reliable communications. Attenuation is a very important factor and will increase with distance and frequency, and as a consequence, longer MV links have to use frequencies in lower bands to guarantee a minimum performance. While it is true that BPL cannot achieve 100% coverage of all links in a typical MV grid (especially in rural areas), measurements have shown that raw data rates of several 10’s of Mbps are possible for links up to 500 m. A general rule-of-thumb is that both older paper insulated lead covered and newer polyethylene insulated cables will support sufficient throughput on cables lengths up to 450 and 900 m, respectively. Measurements have been performed on overhead wires in which it was determined that reliable communications can be supported on links up to at least 2 km. A typical distribution of MV overhead wire and underground cable lengths is shown below in Figure 3. Analysis of actual MV grids in Spain and Switzerland have shown that MV-BPL can therefore cover 90%-95% of the overall grid.

As previously mentioned, the topology of a MV grid can be described as a meshed ring topology in which SSs may have redundant paths to a single or multiple PSs (see Figure 1). This means that SSs will have anywhere from one MV feeder (endpoint) to several feeders per station. For the case of multiple feeders, individual phases (3-phase system) are connected across a common bus bar. Feeder lines are switched within the electrical grid such that a connected tree structure without loops is achieved. Load management and fault isolation can lead to manual or automated switching being performed in the grid. In order to achieve independence from the underlying electrical grid topology, but also to provide increased reliability through redundancy (redundant paths) coupling is generally performed on the feeder side of the switch (opposite the bus bar). This ensures that the logical BPL network topology remains independent of the MV grid's current switched state.

A critical aspect in the large-scale deployment and thereby the scalability of a MV-BPL network is defining a set of suitable guidelines for the cluster planning. In order to provide a scalable solution which can provide BPL coverage of a large MV grid, the network is typically divided into several clusters. As in cellular wireless networks, the communication nodes in a large-scale BPL network must be allocated to different clusters and channels must be assigned to these clusters. Each cluster consists of one master node which connects the cell to the backbone infrastructure, one or more repeaters used for extending the coverage and one or more slaves. Application endpoints may be attached to any BPL node within the network and the BPL network acts as a layer 2 switched Ethernet network. The master is the central node that controls and assigns resources to all the nodes in the network.

All nodes within a single cluster must be configured to operate on the same channel. As there is no BPL technology available which supports dynamic channel allocation between clusters, channels must be manually allocated to clusters such that neighboring clusters operating on the same channel will not interfere with each other. Interference between neighboring clusters can be avoided by using a guard distance between the clusters which are using the same channels. Because of this guard distance, gaps or regions which cannot be covered by BPL may exist in the network (see example in Figure 2). These regions must then be covered by alternative technologies. To increase the amount of channel reuse within the network and minimize the gaps in coverage, multiple channels are used similar to the channel assignment problem known from mobile wireless networks.

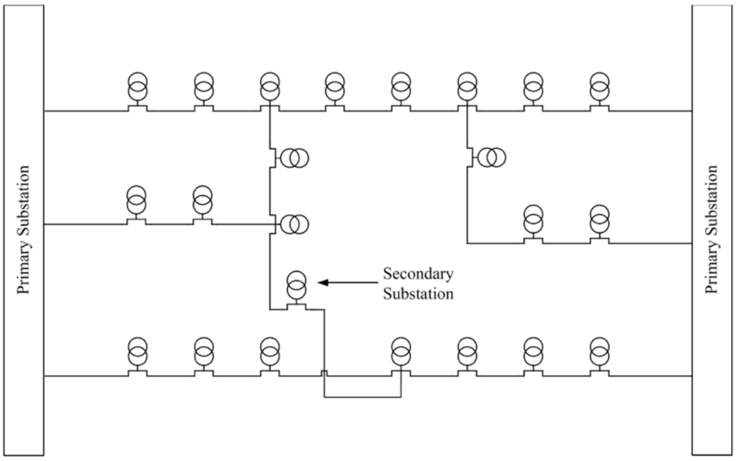


Figure 1: Example of a ringed-mesh topology

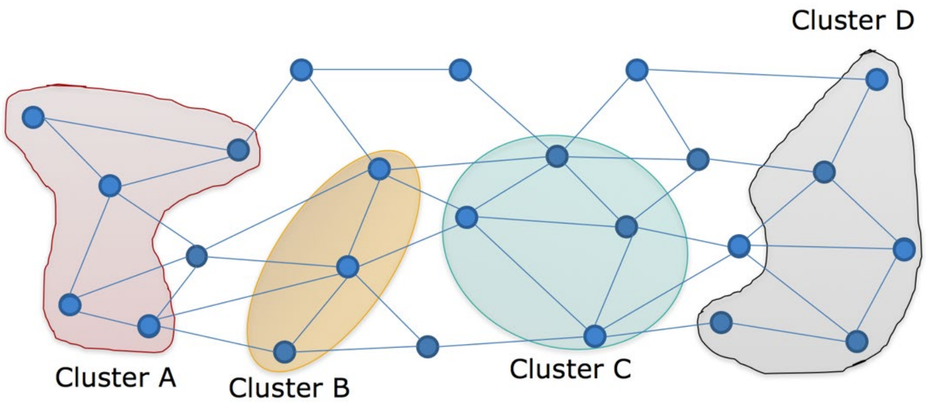


Figure 2: Example MV-BPL clusters in a MV electric grid

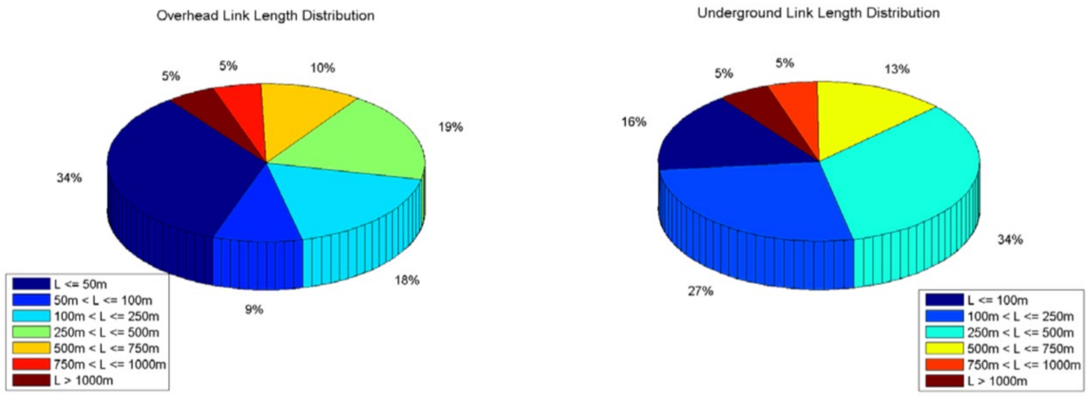


Figure 3: Typical distribution of MV overhead wire (left) and MV underground cable link lengths for urban/sub-urban environments

1.3 Challenge

The motivation behind this project is the development of a new Grid Monitoring & Automation (GMA) solution which takes advantage of the full potential of MV-BPL for enabling MTC-GMA applications in the MV grid. The main driver behind this idea is to provide increased observability and stability to the grid using functionalities previously only used in transmission grids, but for a much lower price that will enable a broad rollout of these functionalities into the distribution grid.

The state-of-the-art in MV automation developments over the last years has provided visibility to the MV grid all over the network, especially with the availability of accurate grid measurements. This visibility allows centralized advanced automatic functions to be realized. The future vision is to provide a synchronized exchange of GMA data from the installed equipment between neighboring SSs which would provide much more value through optimized distributed monitoring, protection and automation functions (PMU, LDP).

The idea is to achieve this through a further development of the MV-BPL technology by enabling MTC-functionality with time synchronization, higher availability and low-latencies permitting the PMU and LDP functionality. The basis for this development is the Power Line data bUS (PLUS) BPL technology which has been developed at the Lucerne University of Applied Sciences and Arts (HSLU). The major advantage being the fact that HSLU has complete control over all aspects of the technology allowing the necessary features and optimizations for such vertical applications to be realized.

In order to achieve the overall goal, the neighboring SSs would be interconnected through this low-latency and high-availability MV-BPL network. The application devices could thus exchange synchronized phasor measurements creating a synchronized monitoring area. This would allow the instantaneous exchange of data and online system analysis of the area to be performed. Furthermore, the LDP application would provide automatic fault detection and mitigation thereby protecting the DNO's important infrastructure and providing higher availability of the electric grid.

The major value of the proposed communication solution with MV-BPL is the low cost. For such functionality – today implemented on the transmission grid level only - a very expensive fiber optic communication would have been required. With the MTC-MV-BPL solution this could be avoided, as the MV lines between the SSs are re-used as the communications medium.

This would lead to a next step in the implementation of MV-BPL clusters. A MV-BPL cluster consists of a number of SSs which are connected together forming a MV-BPL network (see Figure 4 as an example). Within a cluster a single MV-BPL modem will simultaneously act as the network master and serve as a gateway between the MV-BPL network and the Wide Area Network (WAN). The MV-BPL modems within other SSs serve as repeaters or as slaves. The potential for establishing multi-hop communications allows a single MV-BPL cluster to cover a large geographic area. Within this area only a single (typically expensive) connection to the WAN is required rather than a single connection per SS. This reduction in the number of expensive WAN connections provides a further cost advantage for MV-BPL.

Up to now such MV-BPL clusters have been implemented for Automated Metering Infrastructure (AMI). For this use-case, smart meter data is collected by the data concentrator using narrowband PLC technology for the connection between the SS and the meter. The data from the data concentrators in each SS is then further aggregated within the MV-BPL network and transmitted to the head end system through the gateway at the MV-BPL master. The largest current deployment of this solution is in Spain with the utility Iberdrola [1]. However, the network performance requirements for the AMI application are rather relaxed compared to the proposed GMA applications.

Therein lies the challenge. A comparison of the addressed applications is shown below in Table 1. The most critical requirements are highlighted in red. The target of this project is to address the strict latency requirements which are highest for the LDP application (<5 ms). Fulfilling the low latency requirements of GMA applications poses a significant challenge for the communication technology, since a very powerful Modulation and Coding Scheme (MCS) is required for MV-BPL to provide robust communications over the unreliable communications medium. The use of such complex MCS has led to relatively high processing times at both the transmitter and receiver which makes achieving this latency requirement a challenge. Therefore, a detailed research-oriented investigation including simulations within a Model Based Design (MBD) approach was required to optimize the MCS towards minimizing latency. This project has covered a research-based exploration of the optimum schemes and protocols based on the vast experience at HSLU regarding PLC channels, transmission schemes, protocols, etc. A concept and design for an adaptation of the existing schemes and protocols has been developed, mainly based on simulation results tested and optimized on a verification platform.

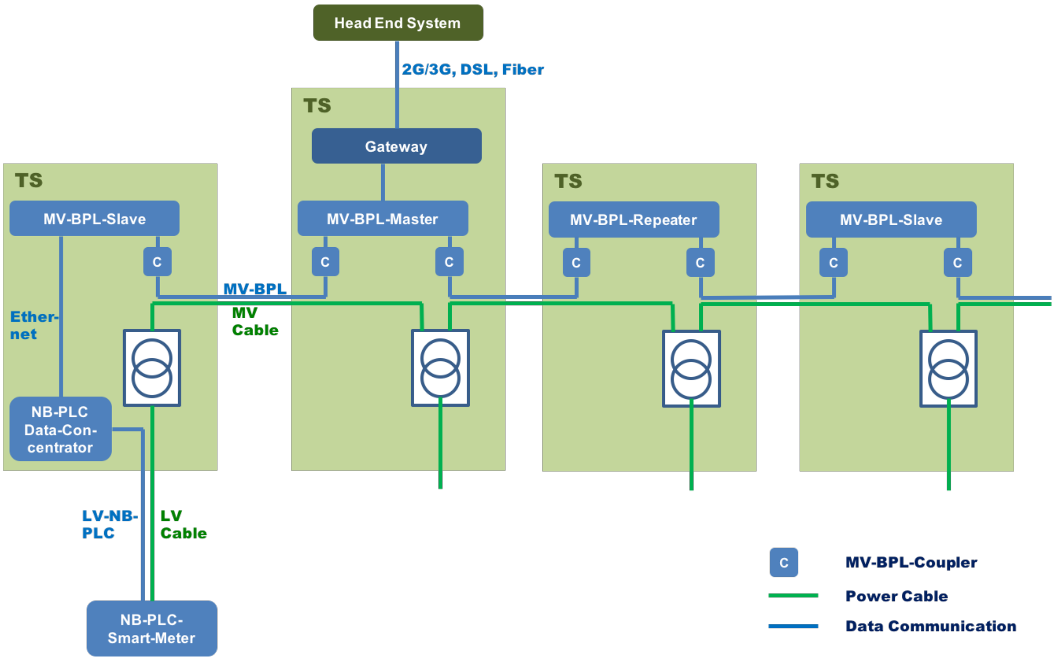


Figure 4: MV-BPL Cluster

Requirement	AMI	LDP	Synchrophasor
Transmission Frequency	Once per day	**Constant transmission of measurement values**	**Constant transmission of measurement values**
Bandwidth	**100 kbps per SS**	10 kbps per SS	65 kbps per SS
Latency	Not relevant (time-intolerant)	**< 5 ms**	< 20 ms
Bit error rate	No specific requirement	**10^{-6} or better**	No specific requirement
Availability	Network must be available for transmission of data only once per day	**99.99% availability**	High-availability if real-time state estimation is performed
Data Integrity	No specific requirements[1]	**100% data integrity[2]**	**100% data integrity[2]**
Time-synchronization Accuracy[3]	Not required	±100µs	**± 3.1µs**

Table 1: MV-BPL performance requirements for smart grid applications

[1] Undetected errors will not lead to a large impact on operations.

[2] The typical definition is a probability of undetected error of 10^{-9} per operational hour.

[3] We assume here that time-synchronization is provided by the network so it is a requirement of the network.

2 Goal of Project

2.1 Main Goal

An investigation will be carried out how Broadband Power Line Communications can be used in the distribution grid which fulfills the communication requirements of Phasor Measurement Units (PMU). The goal is to provide a low-cost communication interface in order to open the door for the more widespread use of PMUs in the distribution network.

2.2 Report Outline

The basis for the development of the MTC-MV-BPL solution is the Power Line data bUS (PLUS) PLC technology developed by the Lucerne University of Applied Sciences and Arts (HSLU). The general architecture and requirements for the MV-BPL technology have been previously described in Chapter 1.2 and Chapter 1.3, respectively. A description of the PLUS technology is provided in Chapter 3. The main application of the area prior to this project has been for avionics systems. The technology has to a certain extent been optimized for this environment (known as PLUS-Avionics). Therefore, the first step in the project was to analyse the technology compared to the PMU application requirements and determine the necessary adaptations and optimizations. This has resulted in a variant of the PLUS technology known as PLUS-Smart Grid. The motivation for the necessary design changes in moving from PLUS-Avionics to PLUS-Smart Grid are described in Chapter 4. Chapters 5 and 6 then describe the adaptations and optimizations in more detail. For technologies for MTC applications it is not only important to consider the high-level design of the technology, but also the processes behind the design and development of the technology. Within this project an optimization to the existing development process of PLUS has also been developed which is described in Chapter 7. Furthermore, security plays a critical role in MTC communications. A security analysis of the MTC-MV-BPL technology has also been performed and is described in Chapter 8. The identified adaptations and optimizations for the PLUS-Smart Grid technology have all been implemented on a set of prototypes. These prototypes are described in Chapter 9. Functional and performance testing has then been performed within HSLU’s *Smart Grid CommTech Testbed Laboratory* which has been developed in conjunction with BKW. In addition to the PMU application requirements, the developed prototypes have been tested for the AMI application against existing prototypes of the iCommUnit product provided by Energie Pool AG. Energie Pool has partially financed the work in this project in order to compare the newly developed MTC-MV-BPL solution against the existing G3-PLC technology in the iCommUnit prototypes. The test setup and results are provided in Chapter 10. Finally, conclusions and next steps for the development of the technology are presented in Chapter 11.

3 Power Line data bUS (PLUS) Technology

3.1 Introduction to Power Line Communications (PLC)

PLC is a wired communication technology that is able to use a Power Distribution Network (PDN) for data transmission by superimposing a modulated high frequency carrier signal over the standard power signal. The PLC signal is modulated completely independent of the underlying power signal, i.e. will function over any DC, AC or even non-energized systems. PLC combines the advantages of wireline communications with the use of an existing (non-dedicated) wiring network. The specific advantage of PLC comes due to the fact that it has been specifically designed for communications over wiring channels that have not been designed for high-speed data communications, e.g. over unshielded wires in noisy environments. Because of its robustness, the PLC technology may be employed to reliably communicate over any shielded or unshielded wired networks that are normally used for low frequency applications such as power lines, telephone lines (twisted pair copper) or low data rate signaling/control lines.

Similar to wireless communications, the term PLC refers to a broad range of diverse communication protocols. Furthermore, as is also the case for wireless communications, certain protocols may be better suited for avionics applications and one should be careful in drawing conclusions based on the analysis of commercial protocols developed for the consumer electronics market. PLC technology is typically divided into two different categories depending upon the band used by the communications signal.

- Narrowband PLC frequencies below 500 kHz can provide maximum data rates up to several 100’s of kbps, however practical and regulatory limitations lead to a more typical achievable data rate of several 10’s of kbps.
- Broadband PLC operates somewhere in the frequency range from 2-80 MHz. Commercial PLC technologies can provide maximum data rates up to 500 Mbps.

What really defines PLC as a technology is the robustness of the communication protocols to the harsh communication channel which exists in Power Distribution Networks (PDN). This mainly involves a multi-carrier transmission scheme in the form of Orthogonal Frequency Division Multiplexing (OFDM) which optimizes spectral efficiency in the presence of a frequency selective channel. Other important features provided by PLC are strong Forward Error Correction (FEC) techniques (e.g. turbo-convolution or low-density parity check codes) to combat impulsive noise. It is these robust protocols that allow high data rates to be achieved over wiring networks not normally supporting data communications such as can be found in PDNs.

3.2 Challenges of PLC

The use of PLC does not come without its challenges. PDNs have been optimized for the distribution of a very low-frequency power signal and are rather unsuitable for high-speed data communications.

The following main factors differentiate the wiring of a PDN from the wiring typically found in data networks

- PDN wiring is typically unshielded.
- PDN wiring will not consist of a twisted-pair but will usually either consist of a single-wire with return over a common chassis or a group of wires routed in parallel. This often leads to a highly asymmetric transmission medium.

- The PDN topology is often tree-like and contains a number of branches or other points at which impedance discontinuities will occur with impedances varying between a few ohms to a few kiloohms.
- The impedance of loads attached to the PDN is optimized for the maximum power transfer of the power signal and is rather arbitrary for higher frequencies.
- Power conversion and other active power elements within loads will generate static and transient noise which will be conducted or even coupled from external sources onto the PDN.

These characteristics lead to a less than ideal communications channel.

- Impedance mismatches will exist at the loads, branching points and other connection points throughout the PDN.
- Each impedance discontinuity will lead to a partial transmission and partial reflection of the PLC signal. At branches the signal power will be split with partial transmission of signal “echoes” down each of the branches. At the receiver these different echoes and reflections will combine leading to highly frequency selective attenuation. Several “notches” or narrow bands which suffer from higher attenuation than adjacent bands will be present. This effect is commonly referred to as multipath fading. As the paths and load impedances between any two transmitters and receivers will vary, so too will the transmission channels vary. This means that the communications channel has a strong dependence upon the location of the transmitter and receiver. Figure 5 shows a typical PLC communications channel. This was taken from a channel measurement on a 400 m section of MV overhead line. The highly frequency selective attenuation with a few deep “notches” is apparent. It is also apparent that the mean attenuation increases versus frequency which is mainly due to the skin effect and dielectric losses from the insulating material.

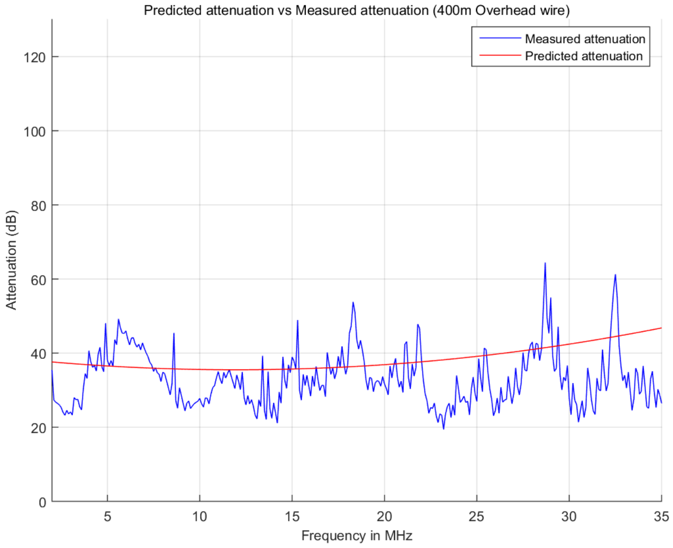


Figure 5: Example PLC channel attenuation for MV overhead line

The PLC communications channel will therefore exhibit the following characteristics

- High transmission signal attenuation (up to ca. 80 dB)
- Frequency selective channel (a channel in which the attenuation varies versus frequency)
- Transient or “bursty” noises exist on the channel
- High power narrowband interference, e.g. from broadcast radio carriers
- Interference from external systems (e.g. adjacent channels) which may be coupled onto the power line due to the fact that it is typically unshielded
- Impedance conditions on the transmission channel may vary versus time, e.g. load impedance changes due to different states of attached application equipment.

It is a common misconception that PLC cannot communicate given these channel characteristics. On the contrary the PLC technology - especially the digital signal processing in the physical layer - has been optimized for over 20 years now to provide reliable communications under these harsh channel conditions. Where traditional data bus protocols would fail, PLC is still able to provide reliable communications.

It is a well-accepted fact that the noise on a power line does not have properties of a “white” Gaussian noise. Typically, three general classes of noise can be expected:

- Colored background noise with a higher Power Spectral Density (PSD) at lower frequencies
- Narrowband background noises which may result from external sources (e.g. broadcast radio) or system internal sources (e.g. application device clock signal)
- Impulsive noise which may be generated from multiple sources at the loads including on/off switching behavior, switched power supplies, etc.

Furthermore, the lack of a shield or twisting of the power cables means that the potential isolation from external effects which may be electro-magnetically coupled onto the power line is reduced. External sources of noise can be other aircraft systems operating within the same (or a nearby) wiring harness, High Intensity Radiated Fields (HIRF) from broadcast radio, low-frequency voltage spikes, lightning, etc.

The main factor influencing the performance of any communication system is the Signal-to-Noise-Ratio (SNR) present at the receiver. Therefore, even in environments with high channel attenuation or high noise, an increase in the transmission signal power could still provide a sufficient SNR. However, within many environments in which PLC is used, the emissions of all devices within the PLC signal frequency range is strictly regulated through Electromagnetic Compatibility (EMC) limits. Even though PLC provides intentional emissions within this band, from the EMC point-of-view it must be categorized as unintentional emissions or noise. These limits mean that the transmission PSD of the PLC signal must be limited in order to be in compliance with the limit for the relevant environmental category.

The fact that the PLC signal propagates over a fixed wiring network means that the channel will exhibit a certain amount of determinism. Time-varying behavior in an installed PLC system typically only result from the time-varying impedances of loads or switching within the network. Proper filter and coupler design can provide a solution which reduces the influence of application device impedance changes on the PLC channel, thereby providing less time-varying behavior. Wireless communication is often considered alongside PLC as a communications technology since it provides many of the same advantages. However, the dynamic propagation environment of a wireless signal poses a significant challenge for the use of the technology in safety-critical applications due to the highly random and time-varying nature of the wireless channel. The determinism provided by PLC is considered to be one of the main advantages for the use of PLC over wireless technology. Table 2 shows a comparison of PLC to other communications technologies.

	PLC	Traditional Data Buses	Wireless
Transmission Medium	Electrical power distribution network	Dedicated wiring	Free space
Harness Requirements	• No data network harness • No change to power network requirements	• Strict requirements for data network harness • Separation of data/power harnesses	• No data network harness • Power network still required
Communications Channel	Mainly deterministic	Highly deterministic	Highly variable
Environmental Susceptibility	Moderate	Low	Very high
Communications Channel Susceptibility	Moderate[1]	Low[2]	Very high
Security	Communications medium inaccessible to attackers	Communications medium inaccessible to attackers	High risk of availability, integrity and confidentiality attacks
Flexibility	Moderate	Low	High

Table 2: PLC vs. Traditional Data Buses vs. Wireless (1) Communications protocols designed to tolerate high levels of noise, (2) Susceptibility achieved through proper wiring harness construction and separation.

3.3 Power Line data bUS (PLUS)

The potential application of PLC for Mission-and-Time Critical (MTC) applications is not new. Previous work by HSLU for avionics applications performed within the EU FP7 TAUPE project has validated the technology up to a Technology Readiness Level (TRL) of 4 [2]. Nevertheless, previous investigations were based on the use of commercial PLC technology and certain deficiencies with that technology had been identified [3]. Unfortunately, the relatively small market segment provided by many MTC applications results in a general lack of support for any necessary adaptations to the commercial technology by the technology suppliers[4]. A “black-box” verification of this technology without support from the technology suppliers would be extremely challenging.

Based on the need for a PLC technology to support the requirements of MTC applications in niche market areas, the development of a dedicated PLC solution was started at the Lucerne University of Applied Sciences and Arts (HSLU) in 2012. The main design goals for the PLC protocol were to maximize reliability, reduce latency and to provide deterministic behavior. These goals are different from commercial technology which includes much dynamic behavior in order to support plug-and-play and high bandwidth applications. The HSLU PLC solution (Power Line data bUS - PLUS) not only targets a communications protocol which meets the necessary functional and performance requirements, but also provides design assurance as is required for MTC applications.

PLUS is the only PLC technology which has been developed specifically for use in MTC applications. PLUS has been designed around:

- Proven standard from other industries for the physical layer (IEEE 1901)

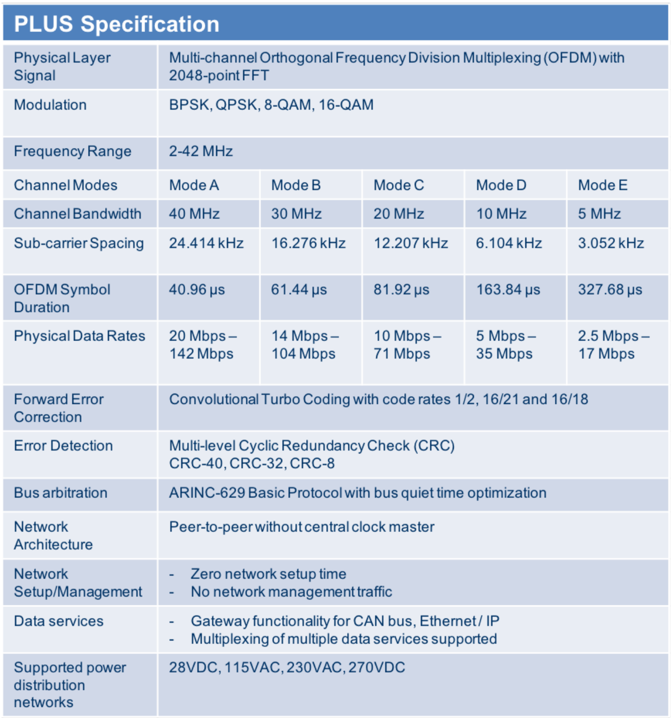
[4] Based on actual feedback from commercial PLC technology suppliers sales quantities of 500’000-1’000’000 are required for them to support new application areas.

- Proven avionics standard for bus arbitration (ARINC 629)
- Custom optimizations and additional protocol layers
- Using available bandwidth to optimize data availability and integrity

The following lists some of the differentiating factors of the PLUS protocol compared to other commercial PLC solutions:

- Bus arbitration is based on a deterministic protocol with no single point-of-failure
- Synchronization for signal decoding (due to asynchronous clocks) is done in a distributed manner, i.e. no central bus/clock master is required
- Error detection is based on optimized techniques from the avionics industry
- Support for multiple independent communications channels through a Frequency Division Multiplexing (FDM) feature
- Robust modes have been optimized for low-latency; robust transport of short messages (< 20 bytes)
- Multiple services can be multiplexed onto a single PLC bus while still providing deterministic behaviour
- Connections are stateless so that the protocol behavior remains static and provides more determinism
- Optimizations have been made to improve susceptibility especially to impulsive and strong narrowband interference, e.g. HIRF

The specification for PLUS Avionics is shown in Table 3.



PLUS Specification					
Physical Layer Signal	Multi-channel Orthogonal Frequency Division Multiplexing (OFDM) with 2048-point FFT				
Modulation	BPSK, QPSK, 8-QAM, 16-QAM				
Frequency Range	2-42 MHz				
Channel Modes	Mode A	Mode B	Mode C	Mode D	Mode E
Channel Bandwidth	40 MHz	30 MHz	20 MHz	10 MHz	5 MHz
Sub-carrier Spacing	24.414 kHz	16.276 kHz	12.207 kHz	6.104 kHz	3.052 kHz
OFDM Symbol Duration	40.96 µs	61.44 µs	81.92 µs	163.84 µs	327.68 µs
Physical Data Rates	20 Mbps – 142 Mbps	14 Mbps – 104 Mbps	10 Mbps – 71 Mbps	5 Mbps – 35 Mbps	2.5 Mbps – 17 Mbps
Forward Error Correction	Convolutional Turbo Coding with code rates 1/2, 16/21 and 16/18				
Error Detection	Multi-level Cyclic Redundancy Check (CRC) CRC-40, CRC-32, CRC-8				
Bus arbitration	ARINC-629 Basic Protocol with bus quiet time optimization				
Network Architecture	Peer-to-peer without central clock master				
Network Setup/Management	- Zero network setup time - No network management traffic				
Data services	- Gateway functionality for CAN bus, Ethernet / IP - Multiplexing of multiple data services supported				
Supported power distribution networks	28VDC, 115VAC, 230VAC, 270VDC				

Table 3: PLUS Avionics Specification

The PLUS Avionics protocol defines Layer 1 and Layer 2 according to the OSI network model. This is further segmented into 5 sub-layers as shown in Figure 6:

1. Physical Layer
    - OFDM based physical layer
    - Based on international IEEE 1901 OFDM standard
2. PHY Convergence Layer
    - Adaptation of MAC frames to physical blocks
3. Media Access Control (MAC) Layer
    - Monitoring of the bus state
    - Scheduling of the transmission on the bus (core algorithm based on ARINC-629)
4. Logical Link Control (LLC)
    - Flow control and multiplexing
5. Data Services
    - Adaptation of one protocol to PLUS (gateway functionality)

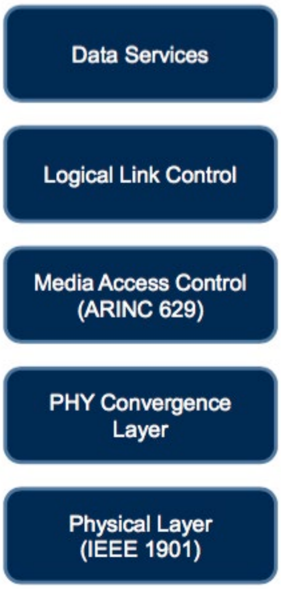


Figure 6: PLUS Protocol Architecture

3.4 PLUS Modem Architecture

An overview of the architecture of a PLC modem is shown in Figure 7. The Digital Signal Processing (DSP) contains the logic implementing the PLC protocol including the implementation of the physical layer (PHY) and Data Link Layer (DLL). The PHY transmitter is responsible for converting the PLC MAC frame provided by the DLL into a PLC signal waveform suitable for transmission on the power line medium. The PHY receiver on the other hand decodes the PLC signal waveform into a MAC frame which is passed to the DLL. The Analog Front End (AFE) provides Digital-to-Analog, Analog-to-Digital and amplification functionality for the analogue signal. The coupler is responsible superimposing the high-power, low-frequency power signal with the low-power, high-frequency PLC signal.

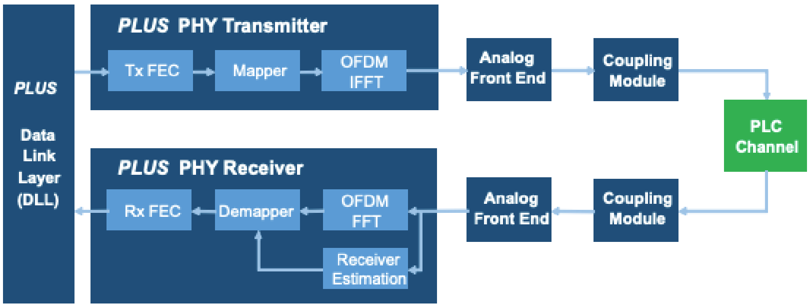


Figure 7: PLUS Modem Architecture

Two different principle coupling methods are available in PLC: capacitive and inductive coupling:

Capacitive coupling

- PLC signal is capacitively coupled to the power line.
- Generally, it provides better impedance stabilization when the impedance of the PLC channel is highly varying.
- Component dimensioning is crucial mainly for high voltage applications (> 400 V).
- The disadvantage is that a galvanic connection to the power line is required (although the PLC modem is typically galvanically isolated with a further transformer.

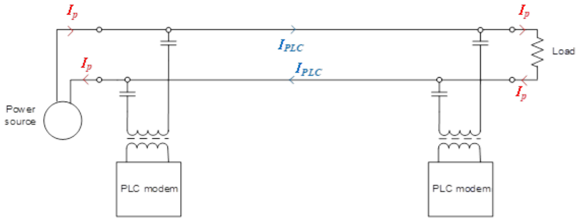


Figure 8: Capacitive Coupling Example

Inductive coupling

- PLC signal is inductively coupled to the power line.
- Galvanic connection to the power line may be avoided if necessary, however capacitive elements (with a galvanic connection) may still be required for filtering.
- Component dimensioning is crucial to ensure that the PLC signal does not saturate with high currents.

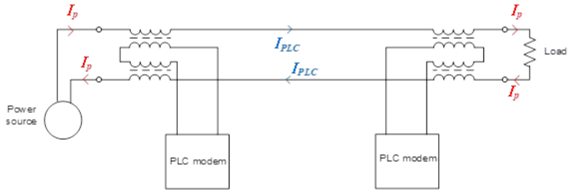


Figure 9: Inductive Coupling Example

Load management and fault isolation can lead to manual or automated switching being performed in the network. In order to achieve independence from the underlying electrical network topology, but also to provide increased reliability through redundancy (redundant paths) coupling is generally performed on the feeder side of the switch (opposite the bus bar). This ensures that the logical PLC network topology remains independent of the MV network's current switched state. Complete independence of the switch state, however, cannot be achieved as the coupler loss will be dependent upon the state of the switch due to fact the impedance seen by the coupler will change during switching. Inductive coupling will generally function better in a closed switch state (low-impedance) and capacitive coupling in an open switch state (high-impedance). The selection of a coupling method is influenced by the cable/wire type as well as the characteristics of the transformer and switch. However, coupler selection may also be influenced by practical limitations such as confined space, safety distance requirements or other installation constraints. Safety regulations will generally require that couplers be installed on non-energized lines.

3.5 PLUS-TimeSync

Within a previous SFOE funded project the PLUS technology was extended in order to support highly accurate time synchronization over a PLUS network [4]. A time synchronization accuracy of ± 0.5 µs over two-hops in a network could be achieved under wide-ranging test conditions. The Time

Synchronization Protocol for PLUS (PLUS-TimeSync), defines a solution for a highly accurate time synchronization between PMU application devices on top of a MV-BPL network. The developed BPL solution with time-synchronization will provide a cost-efficient alternative to existing PMU systems based on fiber optic communications and GPS-based time-synchronization. A system design has been defined allowing each BPL cell to not only synchronize all devices within the cell, but also synchronize to the absolute time outside of the cell.

The end-to-end synchronization has been divided into four different zones as is shown in Figure 10. This hierarchical architecture was selected in order to provide a scalable solution in which an optimized solution is provided for the specific technical characteristics of each zone. This architecture also takes into consideration the cellular nature of a larger BPL network in which each cell is controlled by a MV-BPL master modem. This also allows any loss of synchronization to error conditions to be partially contained within a single zone meaning that the impact will not have a direct impact on the complete system.

Zone A: Synchronization of the grand master clock at the BPL master with the absolute time. This synchronization takes into consideration providing not only a highly accurate solution, but also a solution that is robust against potential security attacks. For that a combination of different technologies are used allowing a sanity check to be made against the obtained time-synchronization and also providing a fallback solution should one of the synchronization sources be lost.

Zone B: Synchronization across the MV-BPL network. The MV-BPL master acts as the time synchronization grandmaster. In order to ensure a standardized BPL solution can be provided this network based synchronization was defined within the framework of the IEEE 1901 BPL standard. Although the standard does not directly allow for a synchronization with the required accuracy the necessary modifications were identified and defined. The required message exchange, however, makes use of management messages which are defined by IEEE 1901 using vendor specific extension fields.

Zone C: Synchronization within the BPL modem between the clocks for zone A and zone C. The synchronization in zone A and zone C is, in principle, running asynchronously. However, in order to provide very high accuracy these two clocks must be synchronized. The developed design takes into consideration the specifics of the target hardware platform which is the Xilinx Zynq System-on-chip.

Zone D: Synchronization to end devices using a standard one pulse per second (1PPS) interface. This provides the most accurate and simple means to synchronize to an end device. Along with the 1PPS signal the absolute time is output as a NMEA sentence. Therefore, the BPL modem always acts as the time master and the attached device is the time slave. This allows the developed solution to interface to existing application devices (even beyond that of the PMU application) without requiring modifications to the devices. This interface is very similar to the absolute time input interface used in Zone A.

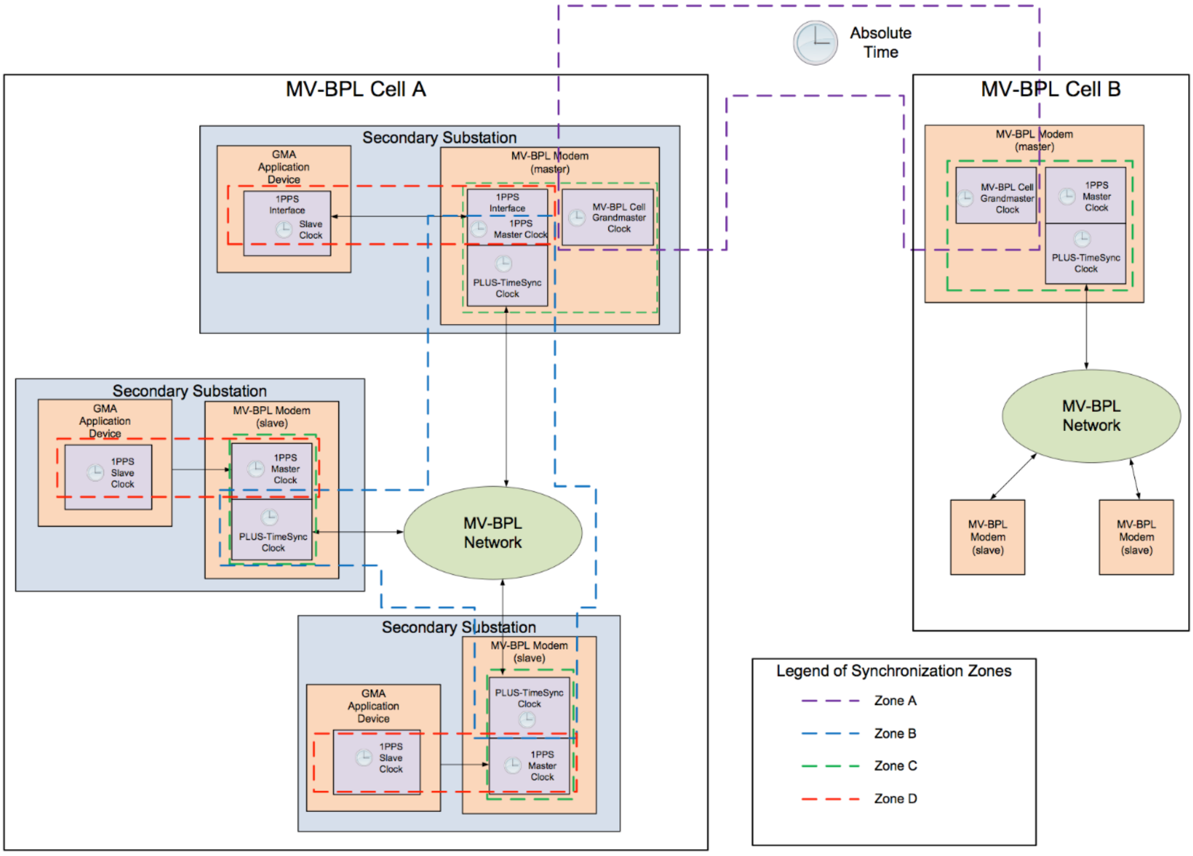


Figure 10: PLUS-TimeSync System Architecture

4 PLUS Smart Grid Design

The main metric for determining the performance of any communications system is the SNR at the receiver. The SNR is dependent upon the transmission PSD, the attenuation in the transmission channel and the noise. Each of those characteristics may be both frequency- and time-variant. The communications channel capacity (rate at which information reliably transmitted over a communications channel) is a direct function of the SNR.

There are a number of performance requirements that an MTC data bus must fulfil. In general, these can be summarized by the five categories presented in Figure 11. The available channel capacity is the main factor for determining if these performance requirements can be met. However, this is presented as a multi-goal optimization problem. Optimizing one of these performance goals will lead to a negative influence on the other goals. Here are some examples:

- Increasing the power will improve the throughput and/or reliability, however it will reduce the EMC
- Using re-transmissions improves reliability, but it reduces the effective throughput and increases latency
- Increasing the number of nodes reduces the effective throughput for each node and increase the latency
- Increasing the throughput can be realized by using higher order modulations (more bits per sub-carrier), however these high order modulations are more prone to errors, i.e. have a low reliability.

Figure 11 captures this design trade-off. It also captures another area of communications system design, namely the deterministic quality of the performance. As previously mentioned, the SNR may be time-variant. This inherently leads to the fact that the performance may also being time-variant. In some application areas it is acceptable if, for example, the throughput reduces to almost zero for a brief time as long as it is very high in the average. For avionics applications this is not the case. Deterministic behavior is required. Achieving deterministic communications system behavior requires proper design consideration. This factor is also captured in Figure 11.

The grey area represents the commercial PLC technology. The design of that technology attempts to maximize throughput which comes at the cost of the other performance metrics. However, the technology is largely non-deterministic meaning that in the best case the throughput may be very high (e.g. several hundreds of Mbps). However, in the worst case the throughput will be very low or even zero. The technology is highly adaptable which inherently leads to dynamic behavior. The spontaneous performance at any point in time can vary within the grey area in this figure.

PLUS follows a different design approach. More weight is placed on maximizing reliability, reducing latency and achieving EMC compliance. In most scenarios it is also necessary to support larger network sizes. Achieving these optimization goals will inherently lead to an overall reduction in the achievable throughput. The solution will also provide deterministic behavior. This is shown in Figure 11 by the fact that the achievable performance area (red band) is much narrower than the grey area for the commercial technology.

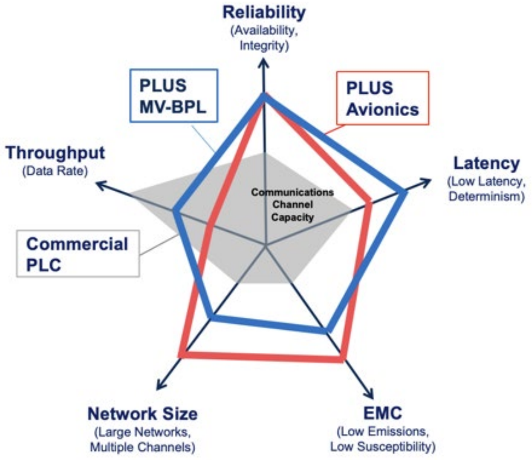

Reliability
(Availability, Integrity)
PLUS MV-BPL
PLUS Avionics
Throughput
(Data Rate)
Latency
(Low Latency, Determinism)
Communications Channel Capacity
Commercial PLC
Network Size
(Large Networks, Multiple Channels)
EMC
(Low Emissions, Low Susceptibility)

Figure 11: PLUS Design Trade-off

5 Latency Optimization

5.1 Latency in Communications Systems

A communication system is portioned in different logic layers according to the OSI model (see Figure 12 and [5]). Latency within a communications network can be defined generically as the time it takes for a packet (or message) to get from the transmitter to the receiver. More specifically, when looking at the OSI model, it is the time it takes for a message to be sent from the application layer of the sender to the application layer of the receiver. This is due to the fact that the application layer is the highest layer responsible for generating and processing communications messages.

Latency can be introduced at each layer depending upon the communications protocol. The main sources of latency associated with each layer are shown in Figure 12 and described here:

A. **Propagation Delay**: The amount of time it takes for the beginning of the communications signal to travel from the transmitter to the receiver. The propagation is a function of the physical distance and the transmission medium. For certain communications technologies like wireless and PLC it is important to not only consider the propagation delay of the direct signal, but also the propagation delay of the different “echoes” or paths other than the direct path which the communications signal traverses. This is due to the fact that the receiver may synchronize to and decode one of these echoes rather than the direct path signal.

B. **Transmission Duration**: In most modern communications protocols the complete data frame must be available at the Data Link Layer (DLL) before it can be fully processed at the receiver. This means that each decoded bit from that frame must be buffered and the frame can only be passed to the upper layers once all bits are available. This leads to the fact that the duration of the overall communications signal must be also considered as part of any delay calculation. The duration can be considered as the time between the very beginning and the very end of the communications signal. This will also include any overhead within the signal which could include preambles, headers, etc.

C. **Hardware Processing Delay**: Almost all modern communications systems will convert the analog communications signal into a digital signal for further Digital Signal Processing (DSP) by the physical layer (PHY). Furthermore, the signal is often times filtered and amplified within the analog domain. This leads to a non-zero delay from the time that the beginning of the analog communication signal reaches the hardware receiver to the time that the digital communications is input into the digital processor for further DSP.

D. **Digital Signal Processing Delay**: The advanced DSP techniques used by modern communications systems means that the time required for the PHY receiver to completely decode all the bits associated with the data frame is non-zero. In other words the last bit from the data frame will not be decoded until a certain amount of time after the end of the communications signal. This difference between the end of the communications signal and the time that the PHY receiver is finished decoding the last bit within the data frame can be considered as the DSP delay.

E. **ARQ Delay**: Typically Automated Repeat reQuest (ARQ) will be used at the DLL which is a means by which erroneous frames are re-transmitted in order to improve the reliability of delivery. The need for re-transmission is determined based on feedback from the receiver through the use of acknowledgement frames. Therefore, the use of ARQ will lead to a delay in two cases. The time for acknowledgements after the transmission of each frame must be reserved on the channel and then the time for re-transmitting the frame (potentially multiple times) until it is correctly received must also be considered. Therefore, ARQ can often lead to a significant (and also variable) delay.

F. **Queuing Delay at DLL**: According to a prioritization concept, multiple queues with different priorities may be used at the DLL. Data frames with higher priority may be transmitted before those with lower priority. Therefore, a delay may be incurred as frames wait within the queue before they are selected for transmission.

G. **Channel Access Delay**: Wireless technologies, PLC and other wired data busses (e.g. CAN) have one thing in common, namely a shared channel. This means that time division multiple access[5] is often used in order to share the transmission channel[6]. Therefore, each transmitter must wait a certain amount of time until the Medium Access Control (MAC) protocol grants it access to transmit on the channel. This waiting time is the channel access delay.

H. **Routing Delay**: In multi-hop networks repeater nodes may need to forward packets at each hop. A routing protocol is required in order to dynamically determine routes through the network. Route setup and maintenance is required and during these times packets may need to be queued for later delivery. Also the forwarding process will lead to additional delays as the packets traverse multiple hops. All these delays can be grouped under routing delay.

I. **Retransmission Delay**: Certain transport layer protocols such as TCP use a retransmission mechanism. This retransmission mechanism will lead to delays similar to that mentioned previously for the ARQ delay.

J. **Queueing Delay at Transport Layer**: Also at the Transport layer queues are typically used. Datagrams may be segmented and require re-assembly which will also lead to delays.

K. **Connection Setup Delay**: Connection-oriented transport layer protocols such as TCP require a connection between sender and receiver to be established. The connection is established through a handshake mechanism which requires a certain time before which datagrams cannot be delivered.

[5] This generic reference to time division multiple access shouldn't be confused with the more specific TDMA protocols.

[6] Some technologies may use a multi-dimensional multiple access method, e.g. also using the frequency or spatial dimensions for multiple access. However, even in this case the time component of the multi-dimensional multiple access will still lead to an overall delay.

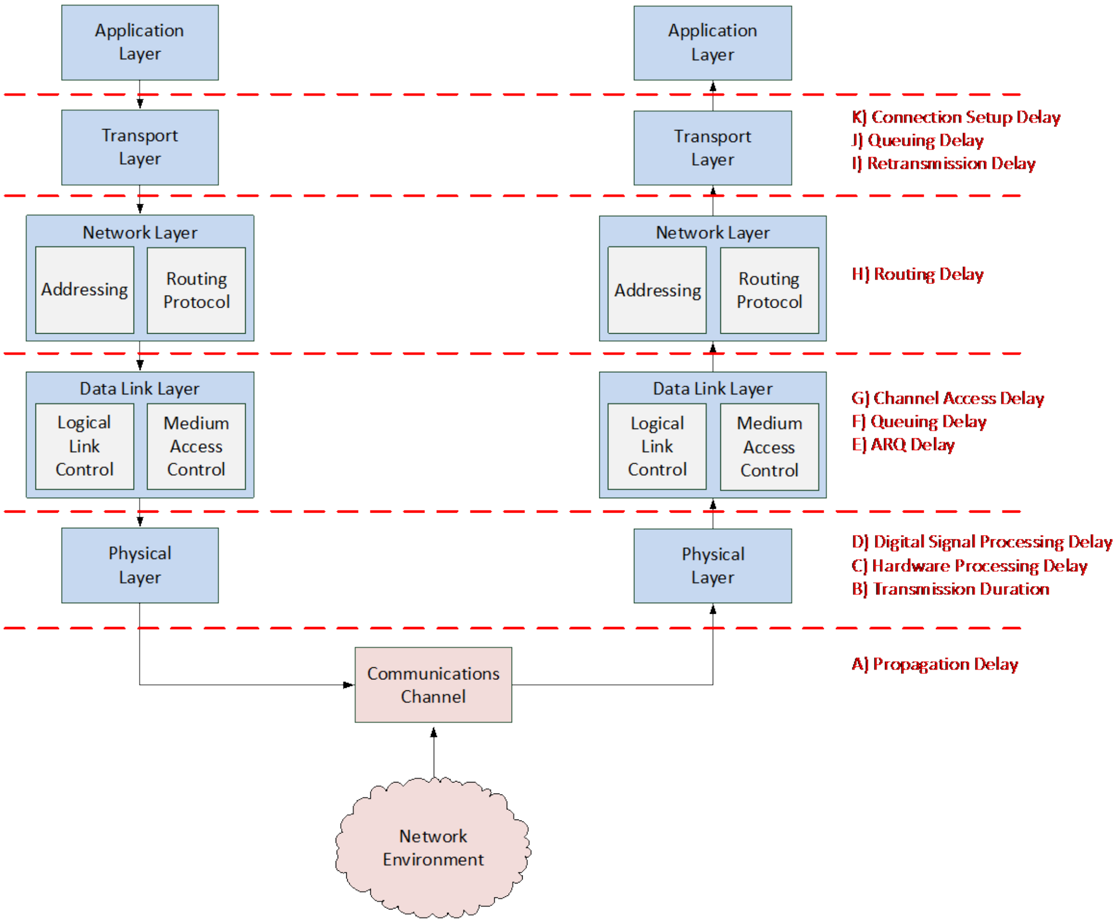


Figure 12: Communication System Delay Sources

5.2 Latency in PLUS

An analysis was performed on the PLUS protocol in order to determine the area in which the maximum improvements in the reduction of latency could be achieved. The targeted areas for optimization within this project are related to (D) – Digital signal processing delay (see Chapter 5.1). This is due to that fact that the interframe-spacing is largely related to the transmit and receive processing delays as is shown in Figure 13:

- Receive (Rx) processing delay: The receiver on each modem must have completed the processing of the previous PHY Protocol Data Unit (PPDU) before it can begin processing the next PPDU. The MAC protocol is responsible for ensuring that this is the case. Therefore, the minimum Inter-Frame Spacing (IFS) must be at least equal to the required Rx processing delay. If this processing delay can be reduced, then the IFS can also be reduced which will result in more efficient bus utilization and, thus, higher throughput.
- Transmit (Tx) processing delay: The MAC protocol of plus works based on a carrier sensing mechanism. Follow-up transmissions are determined based on a certain back-off time after the previous transmission. Therefore, after the previous transmission certain timers will be running which will be used to determine which modem can transmit next and when that

modem can transmit. Once a modem has reached the decision to transmit based on the MAC algorithm, the frame to be transmitted must be sent down through the lower protocol layers (see Figure 6) for further processing before the actual transmission can begin. Due to the necessary encoding and modulation this processing time can be rather significant if not optimized. The MAC protocol must take this Tx processing time into consideration and ensure that this additional delay will not lead to collisions on the bus. This results in higher IFS and, as previously described with Rx processing delay, less optimal utilization of the bus and lower throughput. Therefore, it is also necessary to reduce this processing delay as well.

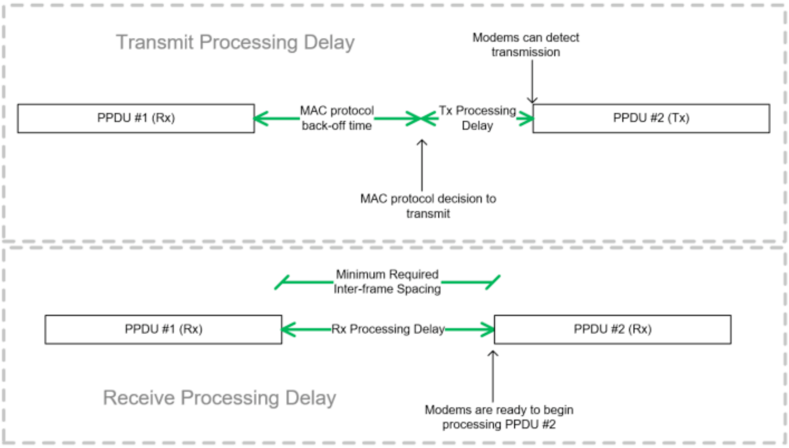

Transmit Processing Delay
Modems can detect transmission
PPDU #1 (Rx)
MAC protocol back-off time
Tx Processing Delay
PPDU #2 (Tx)
MAC protocol decision to transmit
Minimum Required Inter-frame Spacing
PPDU #1 (Rx)
Rx Processing Delay
PPDU #2 (Rx)
Receive Processing Delay
Modems are ready to begin processing PPDU #2

Figure 13: Transmit and Receive Processing Delays

The architecture of the PLUS physical layer (PHY) is shown in Figure 14. Optimizations for reducing the latency have been made in two areas:

1. Transmit processing delay due to the IFFT operation which is located within the TX_SYM block (see Chapter 5.3 for more details)
2. Receive processing delay due to the Forward Error Correction (FEC) based on the Convolutional Turbo Code (CTC) (see Chapter 5.4 for more details).

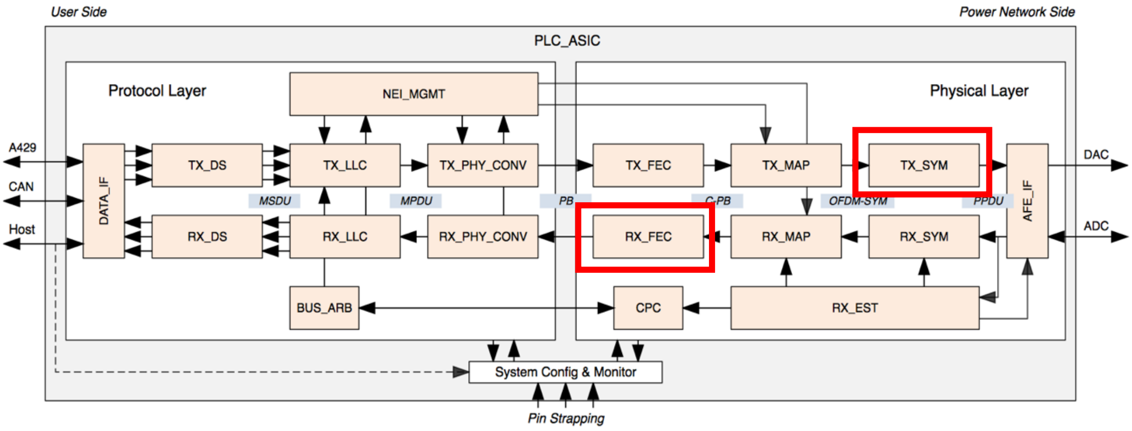


Figure 14: PLUS PHY Architecture

5.3 FFT Latency Reduction

5.3.1 Introduction

The discrete Fourier transform (DFT) is a core component of the PLUS PHY transceiver. Due to the increasing throughput requirements of such systems, an efficient hardware implementation of the one-dimensional DFT is of ongoing interest:

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-j2\pi n \frac{k}{N}} \ , \quad k = 0, 1, \ldots, N-1$$

Existing work in this domain can be broadly divided into approaches based on systolic arrays [6] and those using any variant of the fast Fourier transform (FFT) algorithm [7][8].

[6] specifies two types of OFDM physical layer procedures for broadband communication over power line networks in smart grid, transportation and in-home applications. In situations where strict requirements regarding electro-magnetic emissions must be met, the FFT-based physical layer is preferred over wavelet OFDM since it allows to realizing deep frequency notches without additional transmit filters.

The FFT physical layer version of [9] requires three FFT instances: A combined 4’096/512-point inverse FFT (IFFT) for generation of modulated transmit symbols and preamble mini-symbols, and two separate 4’096- and 512-point FFTs for receive symbol demodulation. All of these are working with the baseband PLC signal. For the specific low-latency FPGA implementation of [9] four different instances of the commercially available FFT core [10] with a target clock frequency of 400 MHz have been used. This core serves as a reference point in the remainder of this text. From the protocol point of view, all four FFT instances could time-share the same hardware in the target PLUS system as they are guaranteed to not be used at the same time during all stages of transmission and reception. However, since the processing pipeline of [10] must be flushed every time, the FFT length N is changed, throughput drops and latency increases beyond the requirements imposed by the system specification, see Table 3. Therefore it was opted for a solution that optimally utilizes hardware resources time-shared between FFT channels.

5.3.2 FFT Processor Architecture

Figure 15 shows the top-level architecture of the proposed solution, which consists of a general-purpose FFT core and the surrounding FFT processor infrastructure. Input data is buffered per channel and forwarded under priority control to the corresponding input of the general-purpose FFT core. Result data is multiplexed to the corresponding channel. Optional output buffers are used for data reordering and sample rate adaptation. The FFT processor functionality can be statically configured for the targeted application. For the PLUS-Smart Grid OFDM system four channels have been used, but the general concept has no such limitation. Each of the channels can be statically configured to any FFT length N supported by the FFT core. This approach assumes that the different FFT lengths required are known a priori, but maintains the maximum FFT core throughput when changing processing from one FFT length to another. This is conceptually different to [10], where the

FFT length can be dynamically changed, but any such change incurs stall cycles and a drop in throughput.

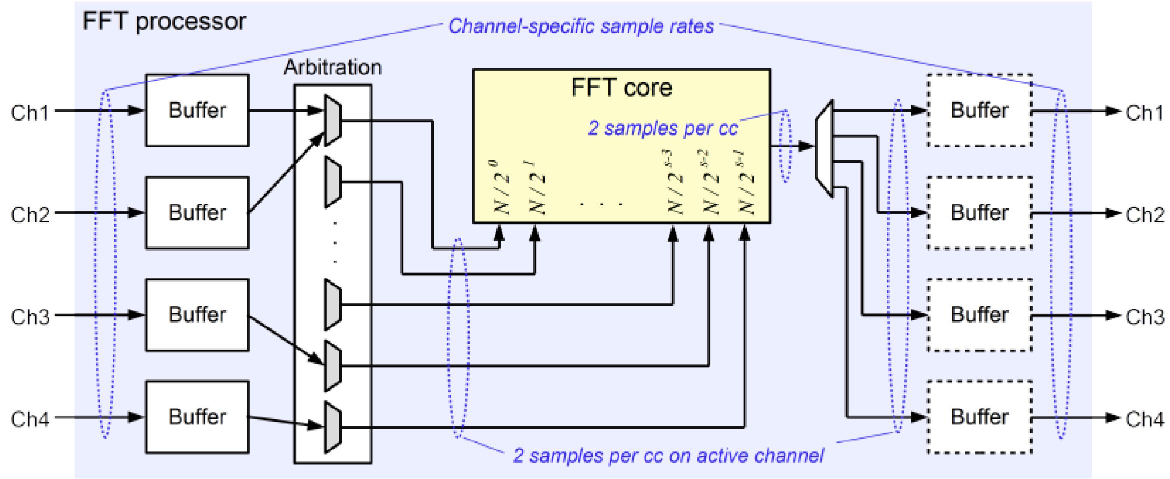


Figure 15: Architecture of the FFT Processor

As indicated in Figure 15, the selected FFT core architecture supports a continuous throughput of two complex-valued samples per clock cycle, which is twice the theoretical throughput of the reference core [10]. The choice of a two-parallel FFT core architecture resulted from a trade-off analysis, which revealed that the linearly increasing hardware cost of higher FFT parallelization is not justified in the OFDM application, because system-level latency would only marginally decrease. Although the particular FFT architecture has been selected based on the requirements of the target application, the FFT core can be reused in various situations, either stand-alone (for single-channel applications) or by making use of the FFT processor infrastructure (for multi- and single-channel applications).

The FFT processor employs input buffers to ensure that once the FFT core has started to process a particular channel, two complex-valued input samples per clock cycle from this channel can be provided to the core. With this method the processing of each channel can be started at the optimal moment in time. This optimal time is the moment when the minimum fill level of the input buffer required for continuous core throughput, independent of the data rate of the specific channel, is reached. The arbitration between channels with different N is handled by the de-centralized control scheme which has been defined.

When two or more channels are configured for the same FFT length, a dedicated input buffer for each such channel is used. These channels are then arbitrated to the same core input. Assuming that the channels input sample rate is high enough, the FFT processor architecture ensures that the maximum theoretical throughput can be maintained at the FFT core output at all times.

Output buffers can be optionally instantiated per channel and used for reordering the bit-reversed FFT core output and/or sample rate adaptation. A channel-specific ID is propagated through the FFT core to allow proper multiplexing at the output buffers.

5.3.3 General Purpose FFT Core

Starting off from the 8-parallel radix-2 multi-path delay commutator (R2MDC) architecture proposed in [11], two modifications were introduced which allow the target throughput of two samples per clock cycle to be maintained even when changing the FFT length N. First, the 8-parallel R2MDC architecture from [11] has been scaled down to the 2-parallel architecture shown in Figure 16 (top) which realizes the target throughput. Moving crisscross elements C2 to the preceding stage prepares for the localized control concept required for continuous throughput. The dummy element C2 added to the last stage does not consume any hardware resources. However, its irregular structure across the log2(N) stages excludes a generic localized control concept for each stage required to maintain maximum throughput. Second, by moving each crisscross commutator C2 into the preceding stage as shown in Figure 16 (bottom), such a control concept becomes feasible. The dummy element C2 added to the last stage does not consume any hardware resources.

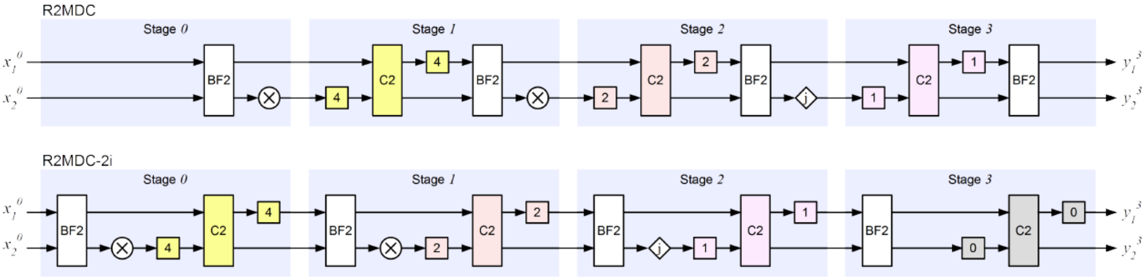


Figure 16: Comparison of the 2-parallel R2MDC (top) and the proposed R2MDC-2i (bottom) architectures for N = 16

The latency L(N) of the 2-parallel architecture is:

$$L(N) = \frac{N}{2} + C_S \cdot log_2(N) + C_W$$

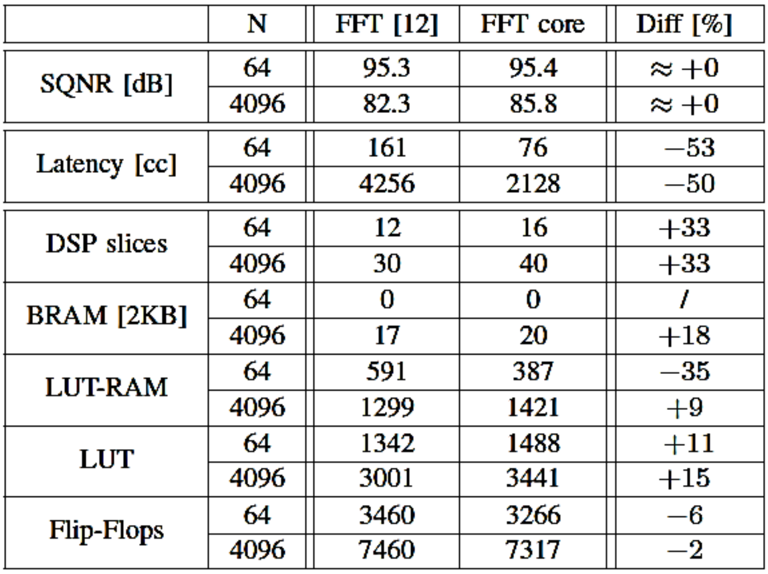
because N/2 clock cycles are required to input all N values, the last of which has to pass through all log2(N) stages for the first result value X[0] to become available at the output. CS and CW are constant values representing the pipelining depth of the data path within each stage and the first twiddle factor generation unit, respectively. In the particular implementation CS = 6 and CW = 8 have been used.

5.3.4 Evaluation on FPGA

The FFT processor and core concepts described above have been implemented in VHDL and integrated into a Xilinx xc7z045-2 device for a target clock frequency of 400 MHz. The twiddle factors are stored with 16-bit resolution and extended to 18 bits on the fly in order to fully utilize DSP slice multipliers. The no-rounding option has been used. The VHDL implementation has been verified using cycle-true and bit-accurate Matlab/Simulink models based on fixed-point numbers. The continuous-throughput feature has been tested by simulating multiple FFTs of different length back-to-back.

Table 4 compares the IP-core which has been previously used ([10]) with new FFT core. All latency and Signal-to-Quantization-Noise Ratio (SQNR) results were obtained by simulation. Hardware resource numbers were taken from FPGA utilization reports of 400 MHz implementation runs. For fair comparison of hardware resource usage, [10] has been configured such as to achieve a slightly lower SQNR as the proposed FFT core.

As expected, the proposed solution reduces latency by a factor of two through its 2-parallel R2MDC architecture. Additionally, the decentralized control scheme guarantees the maximum theoretical throughput even when changing between different FFT lengths. As can be seen in Table 4, the halving of latency and the continuous-throughput feature have been achieved without doubling the utilization of any FPGA resource type. In particular, DSP utilization only increases by one third because of the optimizations that have been developed for the basic computation element of the FFT, called ‘butterfly’. The increase in combinational LUT usage is even less. This is due to the mapping of almost all butterfly logic to DSP-slices, which partly compensates for additional control and twiddle factor generation logic. For N = 4’096, the BRAM and LUT-RAM usage of the proposed solution is slightly higher. This is because the decentralized control concept requires local storage for crisscross elements C2 and twiddle factors, which is difficult to share between stages. For smaller N, sharing is less important, because no BRAMs of fixed size are used. In this case, the proposed twiddle factor generation concept requires less LUT-RAMs than [10].



	N	FFT [12]	FFT core	Diff [%]
SQNR [dB]	64	95.3	95.4	$\approx +0$
	4096	82.3	85.8	$\approx +0$
Latency [cc]	64	161	76	-53
	4096	4256	2128	-50
DSP slices	64	12	16	$+33$
	4096	30	40	$+33$
BRAM [2KB]	64	0	0	/
	4096	17	20	$+18$
LUT-RAM	64	591	387	-35
	4096	1299	1421	$+9$
LUT	64	1342	1488	$+11$
	4096	3001	3441	$+15$
Flip-Flops	64	3460	3266	-6
	4096	7460	7317	-2

Table 4: Difference in latency and FPGA resource usage between reference core [10] and the proposed FFT core with comparable SQNR for N = 64 and N = 4096

5.3.5 Summary

A multi-channel FFT processor that optimally utilizes time-shared FPGA resources has been developed. With regard to previously proposed FFT architectures the work is closest to [11] and [12], but provides the following new contributions:

1. A multi-channel FFT processor that can be tailored to application-specific interface requirements.
2. A decentralized control scheme for radix-2 FFTs that supports dynamically changing N without stall cycles.
3. An implementation of butterfly operations optimized for FPGA-specific hardware resources.
4. A method for efficient twiddle factor storage with on-the-fly resolution enhancement.

It is feasible to double the throughput and cut the latency of state-of-the-art FFT FPGA-implementations by half, without doubling hardware resource utilization and without compromising on the signal-to-quantization-noise ratio. This requires careful selection of the FFT core architecture and several low-level optimizations such as butterfly reorganization for optimal DSP slice mapping and efficient twiddle factor generation. Using a decentralized control scheme, the proposed general-purpose FFT core can be embedded into a multi-channel processor architecture that maintains the maximum theoretical throughput even when the FFT length is changed.

5.4 Turbo Decoder Latency Reduction

The third and final optimization developed within this project is a reduction of the processing time of the turbo decoder. The turbo decoder is part of the Forward Error Correction (FEC) block of the PHY. As previously mentioned in Chapter 5.2 the decoding of the previous frame must be completed in order to begin processing the next frame. The interframe spacing which is in essence a necessary minimum quiet time on the bus must take this processing time into consideration. The major factor currently contributing to this processing time is the time required by the turbo decoder. The decoding of 3 PB520 coding blocks currently requires 500 µs. This means an improvement is required.

Forward Error Correction (FEC) is a common technique of adding redundant coding information at the transmitter which is then used at the receiver to correct bit errors due to channel deficiencies. As such it is a means to mitigate the negative effects of impulsive noise. FEC coding schemes must also be combined with interleaving in order to reduce the influence of burst errors by achieving a time and frequency distribution of the errors which can be better handled by the coding scheme. By using standard uncoded OFDM on a frequency selective PLC channel with impulsive noise, the overall error rate performance will be dominated by the sub-carriers containing the worst SNR. The use of interleaving and coding helps to ensure that the error rate is instead determined by the average SNR of all the sub-carriers. It therefore plays a key role in the presented solution allowing sub-carriers containing a more favorable SNR to compensate for the negative effects of sub-carriers with a very low SNR, without having to dynamically adapt the used modulation and coding.

The FEC scheme is based on a Convolutional Turbo Code (CTC) as defined within [9]. Since their discovery turbo codes have seen widespread use in many communications standards as they provide performance near to the Shannon capacity [13]. As shown in Figure 17 FEC with CTC consists of three different operations at the transmitter. Scrambling helps to give the data a random distribution. Turbo Convolutional Encoding provides duo-binary encoding and supports code rates of either 1/2, 16/21 or 16/18 with block sizes of either 16, 136 or 520 bytes. After encoding the channel interleaving process provides bit-by-bit interleaving to ensure a suitable distribution of coding and information bits across the sub-carriers in the frequency domain. At the receiver descrambling and de-interleaving are simply reverse processes to those at the transmitter. Turbo Convolutional Decoding is an iterative process that uses soft-decisions obtained from demapping to derive binary values for each information bit. The process is based on a Maximum A-Posteriori (MAP) algorithm which is often estimated with the Max-Log-MAP algorithm, which has lower computational complexity. The number of decoder iterations becomes an important parameter with a trade-off between error-correcting performance and latency. However, multiple decoders may be implemented in parallel in order to reduce latency at the cost of more hardware resources. Another parameter to control the performance/resource tradeoff is the number of bits used to represent soft-decision inputs as well as branch and state metrics of the decoding trellis. A detailed analysis and performance evaluation has been performed to find reasonable values for all of these parameters.

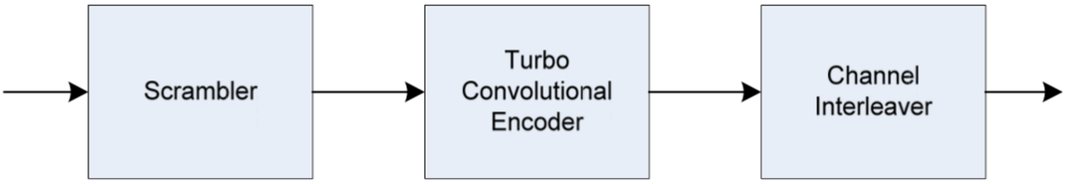


Figure 17: FEC Architecture

According to [14], there are 3 parallelization methods or levels where the turbo decoder can be modified to further raise the decoding throughput, which are:

1. modifications at the turbo decoder level,
2. modifications at the SISO (soft input/soft output) decoder level, and
3. modifications at the Trellis stage level.

In the turbo decoder level (1), multiple dedicated turbo decoders are used to decode multiple codeword blocks independently.

In the SISO decoder level (2), every codeword block is split into several sub-blocks first, and then these sub-blocks are processed by multiple SISO decoders simultaneously.

In the Trellis level stage (3), the functional units inside the SISO decoder are duplicated to complete the computations related to two or more Trellis stages within one clock cycle.

For reducing the latency associated with the module, there are two options:

A. computing the alpha values and the beta values in parallel

B. running multiple engines in parallel for the computation of the gamma, alpha, beta, and output L-values

A drawback of option A is the necessity to store all the beta values in memory (like the alpha values), thus increasing the memory requirements.

Option B is straightforward for the computation of the gamma values and the output L-values. The parallel engines computing the alpha values and the beta values operate on overlapping memory areas (because of the traceback), but this does not pose a problem.

While Option A yields a certain improvement, namely a reduction of the computation time by a factor 0.7 or 0.8, Option B has a much greater potential. Theoretically, with a sufficiently large number of parallel engines, the computation time can be scaled down by a factor 100. However, this would require about 500 engines working in parallel.

Given the hardware resource constraints of the ZYNQ SoC prototype-platform, a parallel Turbo Decoder architecture using a combination of the optimization options 2 and B listed above has been designed. This design uses 4 parallel engines as shown in Figure 18.

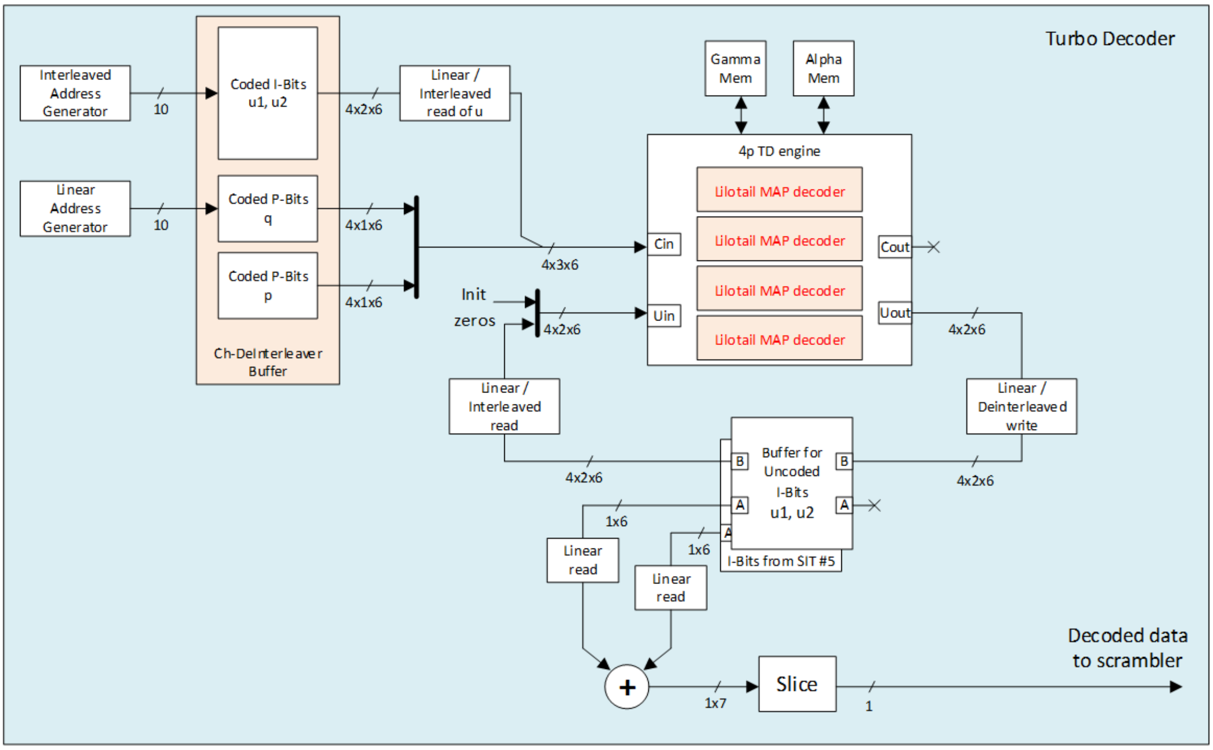


Figure 18: Parallel Turbo Decoder Architecture

Figure 19 shows an initial simulation of the BER performance of the turbo decoder (PB520, 3 iterations) with and without parallelization (16 parallel engines) for binary signaling over an AWGN channel. Additionally, the performance of a rate 1⁄2 convolutional code (the one used in IEEE 802.11) is shown for comparison purposes. It is apparent that the parallelization has no effect on the performance.

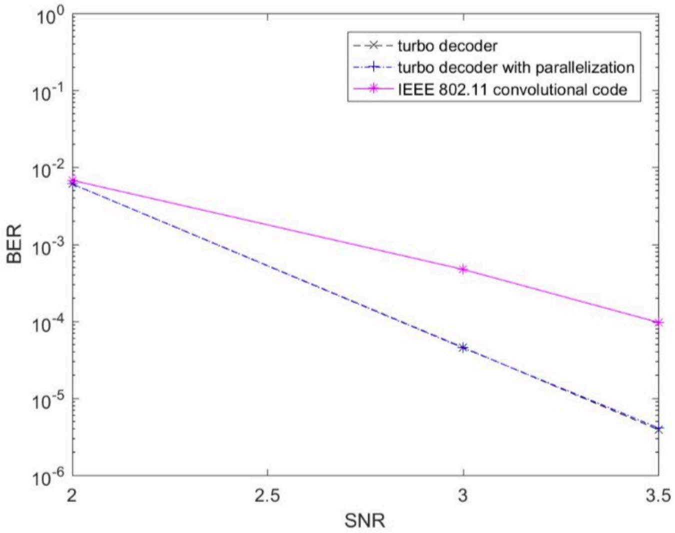


Figure 19: Simulation result from turbo decoder parallelization

The next step was to realize the full algorithm for parallel turbo-decoding in the PLUS PHY simulation platform (PhySimPlatform) which realizes all the main components of the PLUS PHY (see Figure 14). It allows multiple variants of different algorithms to be compared against each other as is shown in Figure 20. Also, the algorithm implemented in MATLAB which was used for initial simulations can be compared against the final hardware implementation which has been implemented using Xilinx System Generator. Figure 21 shows a BER curve comparing the performance of the original turbo-decoding algorithm (blue) against the optimized parallel turbo-decoding algorithm with 4-parallel engines (cyan). As can be seen the performance remains the same for the newly implemented algorithm. However, a reduction in the processing time has now been achieved from 500 µs to 150 µs (a factor of 3.33).

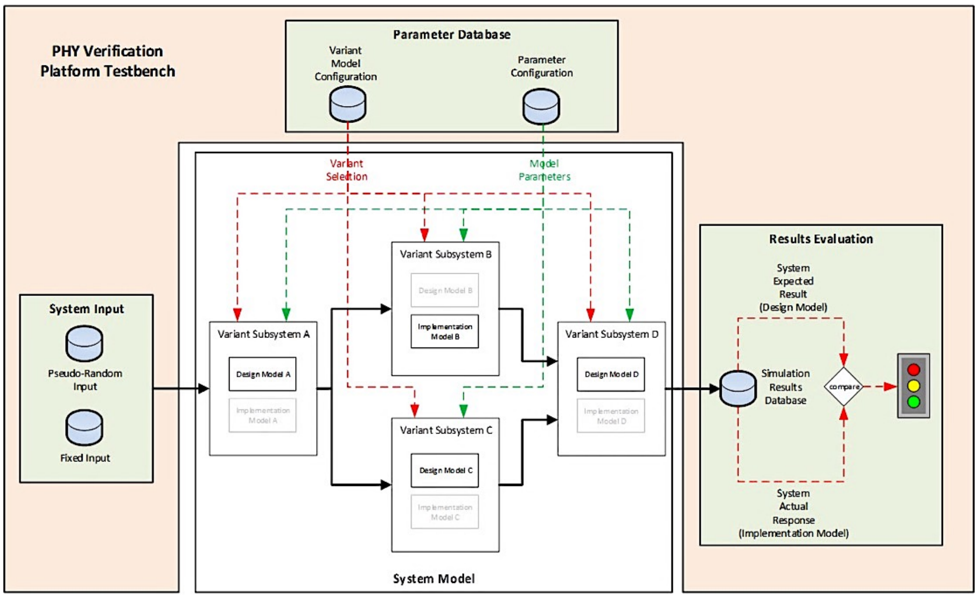


Figure 20: PhySimPlatform Verification Testbench

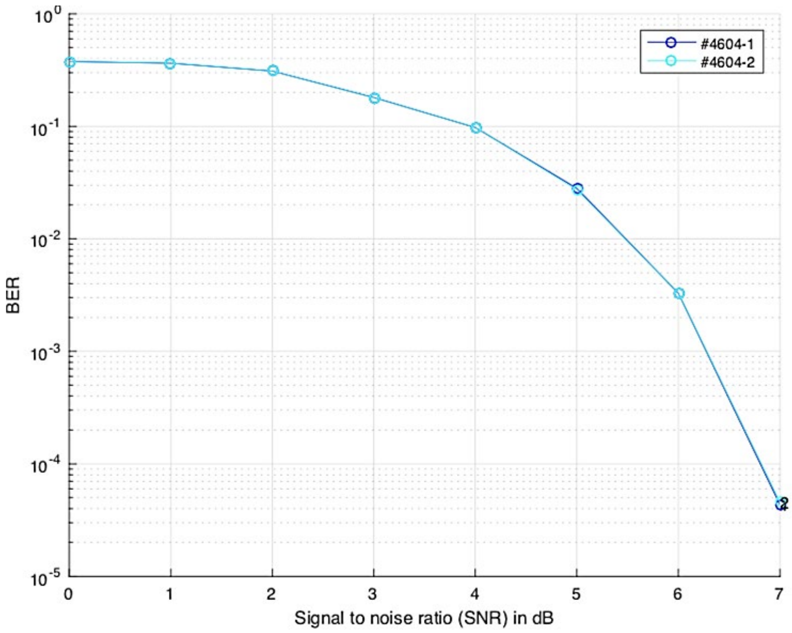


Figure 21: Turbo Decoding Performance Comparison

The following conclusions can be drawn:

- With parallelization, it seems possible to reduce latency by a factor of 3.3. The achievable reduction depends on the number of parallel engines one can afford. An analysis of the available hardware resources showed that up to 4 parallel engines could be implemented within the existing PLUS prototype.
- The BER performance does not suffer from the parallelization and there is no necessity to run extensive simulations with a parallel decoder version.
- With our rate 1⁄2 turbo code we reach 10^{-5} at about 3.3 dB for binary signaling over an AWGN channel. With a theoretical Shannon limit at about 0.2 dB, this is a bit more than 3 dB away from the channel capacity.
- The turbo code clearly performs better than a common convolutional code, which can be seen by steeper BER curves.

5.5 Higher Order Modulation

The use of OFDM for the PLUS PHY allows different modulation per sub-carrier to be used. One unique trait of the PLUS technology is that the modulation per-subcarrier is statically configured. Typically, commercial BPL technology will use adaptive bit-loading in order to select the optimal modulation scheme based on the estimated channel SNR. This dynamic bit-loading can lead to an optimum throughput given a specific channel. However, if channel conditions change, then the new channel SNR must be re-estimated, a new modulation per sub-carrier (known as a tone map) must be selected and the tone map must be reliably exchanged with the neighboring modem. This type of dynamic bit-loading suffers from several drawbacks for MTC applications:

- Changing channel conditions can lead to very poor performance until the bit-loading process again reaches an optimal state. For consumer applications (e.g. inhome networking of consumer electronics which is the prior target of commercial BPL) this is not so critical as the average performance is the important measurement criteria. For MTC applications the worst-case performance is instead the important measurement criteria.

- An optimal tone map is anyway only valid for the unidirectional channel between two modems. Therefore, it cannot be used for broadcast traffic. Again, consumer applications typically consist of a majority of unicast traffic. MTC applications typically use a majority of broadcast traffic.
- Determining the optimal tone map during dynamic bit-loading leads to additional connection setup delays which will increase the latency.

Due to these disadvantages PLUS has focused on providing an optimal solution for a static bit-loading. However, until the beginning of this project PLUS for avionics applications has only supported the following modulations per sub-carrier: BPSK, QPSK, 8-QAM and 16-QAM. Support for higher-order modulations has now been developed for PLUS-SmartGrid. The PLUS PHY has been extended to support the following modulations: 64-QAM, 256-QAM and 1024-QAM. On one hand the use of higher order modulations will increase the potential throughput of the PLUS PHY. However, it will also decrease the latency. Figure 22 shows the mapping of an Ethernet frame down to a Physical Protocol Data Unit (PPDU). After performing block encoding of Physical Blocks (PB) the resulting MPDU is mapped to one or more OFDM payload symbols. The higher the modulation the more bits can be mapped to each sub-carrier. The time duration of each OFDM payload symbol remains fixed (see duration times in Table 5). Using higher order modulations generally allows more bits to be mapped to a single OFDM payload symbol which results in less OFDM payload symbols being required which reduces the duration of the PPDU and will therefore decrease latency.

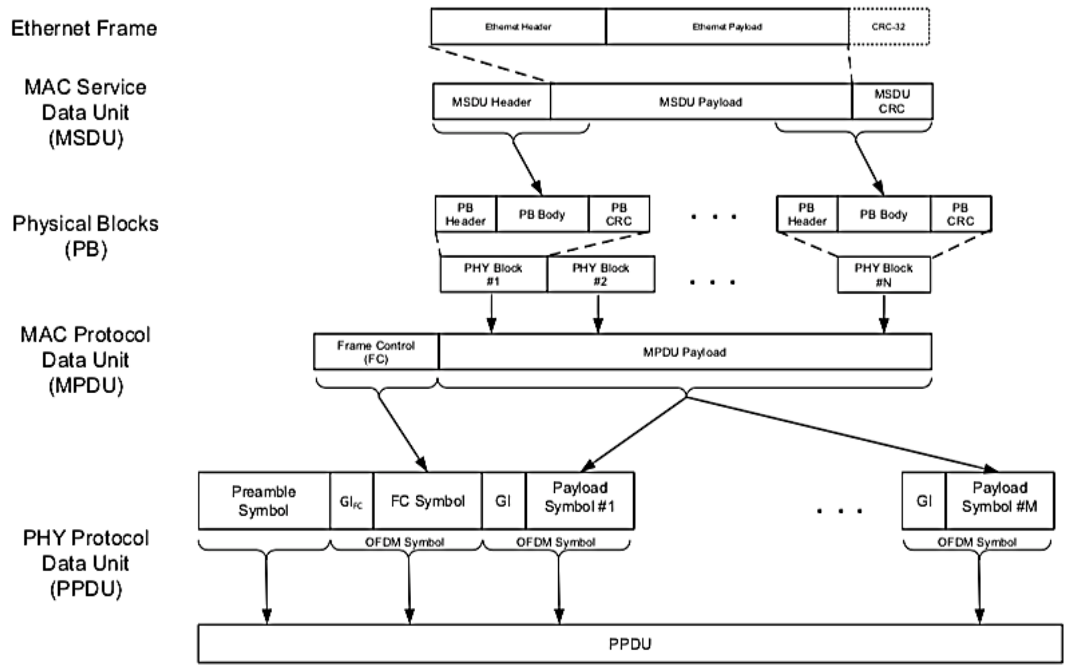


Figure 22: PLUS Transmit Framing

6 Network Support

6.1 Overview

In Chapter 1.2 the general topology of a MV network has been described. This topology is a ringed mesh in which SSs may have redundant paths to a single or multiple PSs (see Figure 1). The potential presence of multiple feeders connected across a common bus bar means that a PLC signal injected at one SS may propagate in multiple directions (through each feeder cable), but also over across a SS without the use of repeaters[7], thereby creating a broadcast channel (see Figure 23-left). On the one hand, the broadcast nature of the PLC signal in a MV network provides the potential for increased redundancy both through multiple paths (feeders) as well as across multiple hops along a single feeder (see Figure 23-right). If a cable fault occurs, data may be routed across an alternative path or if a node failure occurs an intermediate node may be used as a repeater. This is a very important aspect for Smart Grid communications in order to increase the network reliability against node and link failures. On the other hand, the interference domain of a SS may be rather large which can reduce the potential for resource reuse in the network. This problem is further complicated by the previously mentioned parallel cables in a common duct which leads to the fact that SSs located a large number of "hops" from each other may still exist in each other's interference domain. The size of the broadcast domain for each node may change dynamically over time as the channel conditions and network switch state changes. With the commercial BPL technology there is currently no practical method available for limiting the interference domain size other than reducing the transmission power spectral density. Coupling to alternating phases on neighboring links has been previously investigated within the STAR project [1], however has been found to only provide minimal signal attenuation.

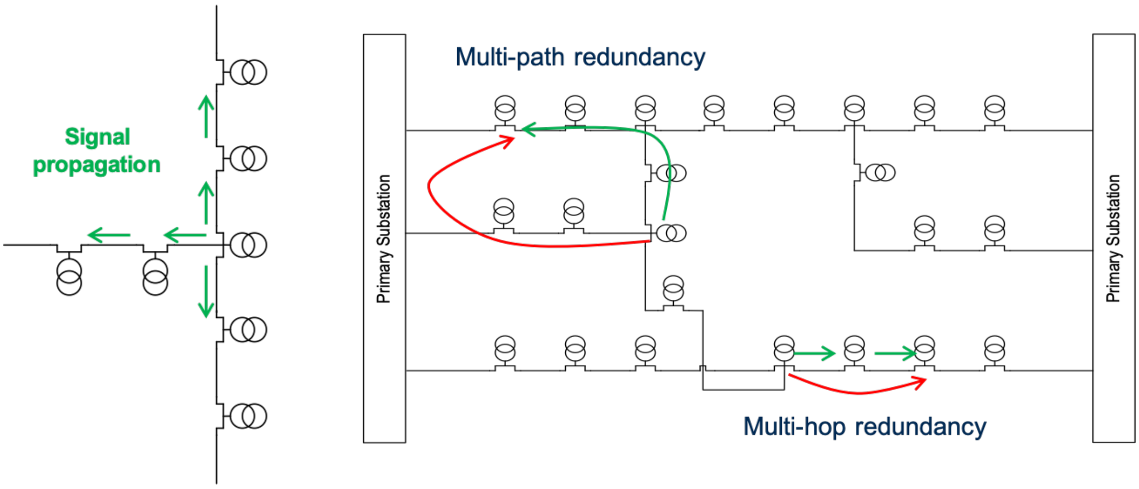


Figure 23: MV-BPL Signal Propagation (left) and Multi-path/Multi-hop Redundancy (right)

[7] The feeder cables emanating from a single SS are connected together across a common bus bar. This bus bar has been found to provide relatively little attenuation for the BPL signal (ca. 5 dB). This leads to the fact that the BPL signal will propagate from one feeder cable to the next thereby extending the transmission range beyond that of just the neighboring SSs. Of course, the attenuation will still eventually be high enough to limit the signal propagation distance.

An additional factor critical for achieving a highly scalable MV-BPL solution is the use of a cellular network architecture. With the cellular approach different logically independent cells are defined as a collection of neighboring SSs. One or more modems within each cell are designated as masters and provide gateway access to the Wide Area Network (WAN). Neighboring cells are then assigned orthogonal frequency channels such that they can operate independently of neighboring cells. This general architecture is used within the to-date largest MV-BPL deployment by Iberdrola within the STAR project [25].

The presence of relatively large broadcast domains as well as the necessity to support multi-hop repeating in the MV network makes investigating MV-BPL at the network level so important. Medium Access Control (MAC) and repeater techniques as well as the proper selection of network architectures become critical. Achieving application performance and high availability requirements with the limited available resources requires a high level of network wide resource reuse combined with techniques which can take advantage of the available redundancy within the network. The PLUS technology for avionics applications does not support multi-hop networks as it is not required. The relatively small size of the aircraft means that all modems within a single PLUS network are part of a single broadcast channel, i.e. they can all “hear” each other. Multi-hop connections with repeating are not required. Therefore, for MTC-MV applications the PLUS technology has to be adapted in order to support multi-hop connections as well as multiple channels.

6.2 Multi-hop MAC Protocol

A MAC protocol is required which supports the following main attributes:

A. Low implementation complexity: highly dynamic and complex algorithms/protocols are available which solve the problem. However, the common factor among all successful MTC data busses is their simple implementation. This simplicity provides deterministic behavior and allows implementations to be certified for safety-critical applications.

B. Packet loss must be tolerated by the protocol

C. The protocol cannot provide a single point-of-failure, i.e. it must recover when one or more modems would fail.

D. The protocol should provide plug-and-play functionality.

E. The protocol should reliably support broadcast transmission even in the presence of the Hidden Node[8] problem.

F. Optimally the MAC protocol should inherently support repeating. Spatial re-use of the channel is not a must, i.e. it would be OK if only one modem per network transmits at a time even if spatial re-use would be possible.

G. The protocol should support open-loop control logic where possible.

Many different MAC protocols exist as are shown in Figure 24. Protocols can generally be divided into random/stochastic protocols and controlled/deterministic protocols. Furthermore, protocols can be categorized whether they are centralized methods requiring a central master node in order to operate or distributed protocols in which each node can act in a peer-to-peer manner. The ARINC-629-based MAC protocol (CSMA/CP) in PLUS provides a very good solution for networks in which each modem can hear every other modem. Channel access can be reliably regulated within the need to have a master and packet errors will not influence any further transmissions beyond the current transmission.

[8] A node is visible to an access point, but not to other nodes communicating with that access point.

The problem is that this protocol requires a static configuration per modem, i.e. it does not support plug-and-play behavior. It also does not provide a suitable solution in the presence of the Hidden Node problem [26].

Pure CSMA/CA suffers from the potential for collisions as multiple modems contend for the medium. This problem is typically mitigated by the use of re-transmissions in case of a collision (ARQ). However, ARQ cannot be used for broadcast traffic (which is the majority of traffic for MTC applications). Collision detection schemes using full-duplex transceivers cannot be reliably used for PLC due to the high dynamic range. TDMA protocols suffer from low efficiency when modems do not have any frames to send within their time slot. In scenarios in which the offered traffic by each modem is very asymmetric and aperiodic a CSMA/CA protocol provides higher efficiency because each modem only contends for channel resources when it has traffic to send. Adaptive/dynamic TDMA schemes are available such as implemented within the BPL OPERA standard [32]. However, determining the offered traffic from each modem and determining the optimal TDMA schedule can be very challenging and error-prone.

TDMA like polling schemes exist which are similar to Token Ring protocols. A master sends a “poll” control message to a slave. The Point Coordination Function (PCF) in IEEE 802.11 is such a protocol. Polling is used within the Contention Free Period (CFP). The AP maintains a poll list and sends a control message to each slave within that list. The slave for which the control message is destined can then either transmit or send a NULL frame. Polling schemes suffer from the necessary overhead in order to transmit the control messages required for polling.

More interesting is a contention period multi-poll mechanism (CP-Multipoll) such as proposed within [27]. With these schemes the random backoff values are defined by the master for its slaves. The values are then distributed in a poll message from the master to a number of slaves. The slaves then contend for the channel based on the distributed backoff values.

A new MAC protocol has been designed in this project, PLUS-TokenRing, which is a hybrid solution between a pure adhoc CSMA/CA solution and a pure Token Ring solution. The overall network architecture is shown in Figure 25. At the center of the architecture is a token ring which consists of the grandmaster (blue) who is responsible for managing the token and a number of master nodes (red). The token is passed around the ring formed by these nodes. A second level of the architecture is then available in which one or more slave nodes can be associated to each of the master nodes within the ring. The master and its slaves then comprise a CSMA region in which channel access is based on the CP-Multipoll mechanism mentioned above. The two-level hierarchy provided by this architecture thus supports higher scalability. It also means that the token does not need to be passed to every node in the network meaning that the round-trip time of the token can be reduced which will reduce the overall latency. Also, the CP-Multipoll mechanism used within a single CSMA region allows the master to assign static backoff timeslots which reduces the probability of collisions and provides more deterministic behaviour. The latency-critical data is exchanged between neighboring SSs. This architecture allows that data to be exchanged directly within each CSMA region.

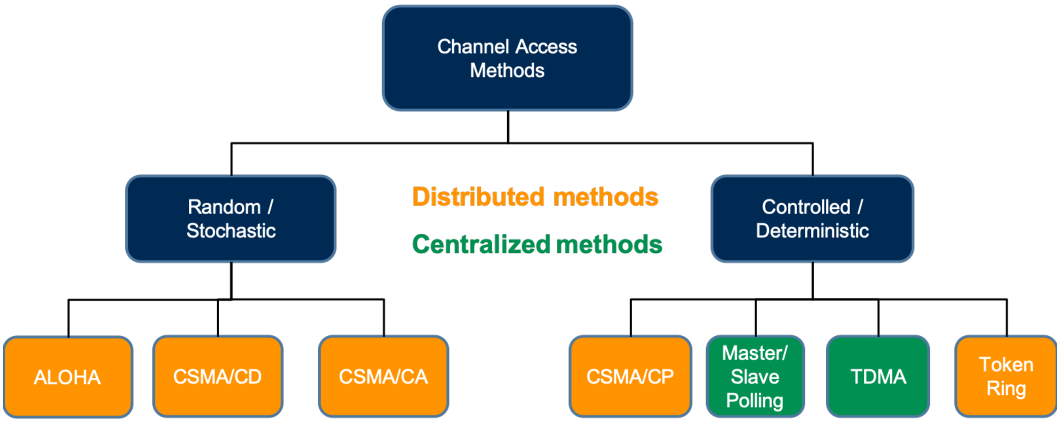


Figure 24: Channel Access Methods

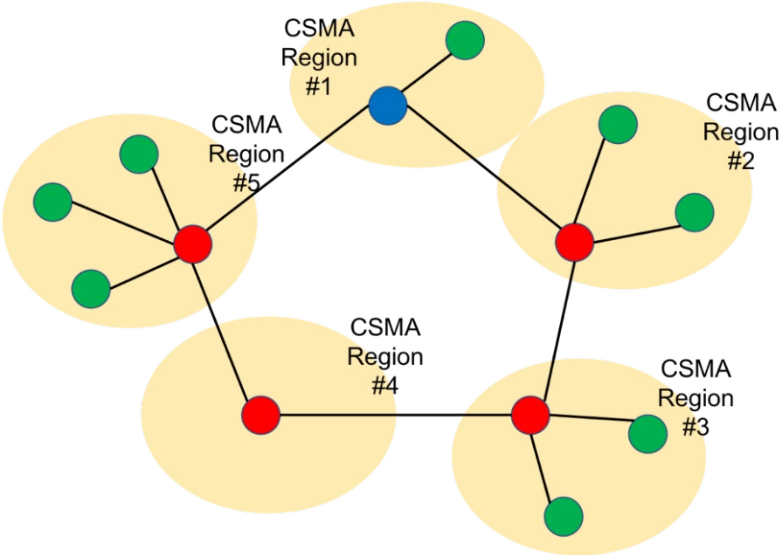


Figure 25: PLUS-Token Ring – Logical Network Architecture

6.3 Multi-hop Routing Support

The Multi-hop MAC concept presented in the previous chapter is responsible for managing the channel access, i.e. determining which modems within the multi-hop network are allowed to send at which time. However, in addition to the multi-hop MAC protocol a multi-hop routing process is required. End-to-end routing with PLUS means that there is a need to route Ethernet frames from the source attached application device to the destination.

The MV-BPL network must emulate a virtual switch connecting all MV-BPL modems as is shown in Figure 26. This means that all MV-BPL modems within a single cell will appear to be connected across a local link and are unaware of the underlying topology. This also means that any routing or management messages are transported using Ethernet frames and that the routing protocol should work without manipulating any OSI Layer 3 routing tables. It is further not required for the MV-BPL networking functionality that the MV-BPL modem has an IP address. This allows any IP protocol (e.g.

IPv4 or IPv6) to run on top of the MV-BPL network, allows an easier integration of application devices connected to the MV-BPL modems and means that broadcast/multicast protocols are also supported without the need for additional L3 multicast routing protocols.

As will be described in Chapter 6.5 a MV-BPL modem will interface to one or more Smart Grid application devices through an Ethernet-based LAN. This means that the MV-BPL network will be used as a bridge between distributed LANs. All Ethernet frames shall be passed transparently through the MV-BPL network. Frames must be first passed through a MV-BPL bridge (modem) between the external LAN and the MV-BPL network. At this point, the next destination may be another MV-BPL modem (shown in the figure as a station) or directly another BPL bridge. The frame may potentially travel through a number of MV-BPL modems on its way to the other MV-BPL bridge. At the MV-BPL bridge, the bridge will pass an Ethernet frame towards the final Ethernet station destination.

Each MV-BPL modem is required to maintain a bridging table including the Ethernet stations attached to its attached LAN as well as other Ethernet stations attached to other MV-BPL modems within the MV-BPL network. This bridging table is maintained through listening to Address Resolution Protocol (ARP) messaging (also known as ARP snooping). This requires that ARP messages are flooded throughout the BPL network and then transparently into the attached Ethernet networks of all BPL bridges.

One further concept that is introduced is a gateway to the WAN or backhaul network. This is shown in Figure 26 as the Gateway Bridge (GB). While the figure shows a single GB, multiple GBs may exist in a network.

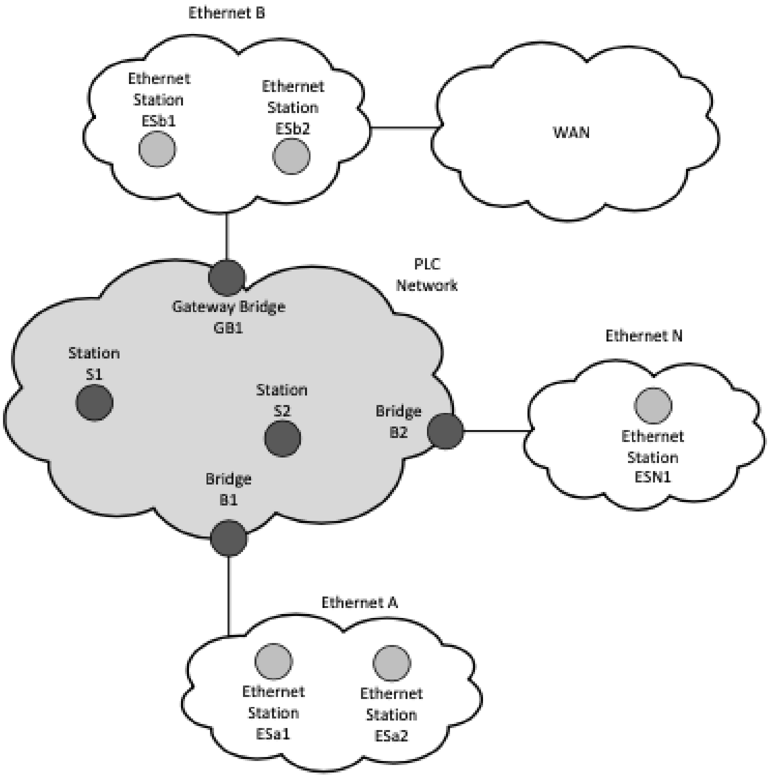


Figure 26: PLC virtual bridging of Ethernet networks [9]

Selective repeating/forwarding of multicast/broadcast frames is required in order to mitigate the Broadcast Storm problem [33]. The Classical Flooding (CF) algorithm is to use Duplicate Packet Detection (DPD). With DPD each route will forward each multicast packet only once. With DPD two main methods are possible: sequence-number based DPD and assisted hashing DPD [30]. In [30] an analysis showed that sequence-number DPD is superior in terms of scalability, efficiency, energy consumption and bandwidth. In [31] a sequence number length of 16 bits (2 bytes) is recommended.

For PLUS it has been decided to use DPD for multicast forwarding. Each modem will maintain a sequence number counter with a size of 16-bits. Each newly generated multicast MSDU will be tagged with a multicast sequence number (MCAST_SEQ_NUM) and the sequence number will then be incremented. When a modem receives a MSDU it will use the MCAST_SEQ_NUM in the MSDU in order to perform DPD. A cache of all previously forwarded multicast MSDUs from each source modem will be maintained. If the MCAST_SEQ_NUM for a given source is not found in this cache, the MSDU will be forwarded and the MCAST_SEQ_NUM along with the source address will be entered into the cache. If the MCAST_SEQ_NUM for the given source address would be found in the cache, then the packet is not forwarded.

The question then remains how large the cache window for each source address should be. Theoretically, each modem could maintain a cache with the maximum MCAST_SEQ_NUM space which would be 2^{16}. However, this approach has two disadvantages. The first is when the MCAST_SEQ_NUM would wrap around. The forwarding modem would think that it has already forwarded these very old MSDUs even though they are really new MSDUs from the wrap around. The second disadvantage is when a modem restarts. If it would start sending multicast MSDUs with MCAST_SEQ_NUM's which are within the existing cache window of the forwarding modems, then these modems would discard the new MSDUs (generated after the restart) thinking that they are actually old MSDUs (before the restart). It is just advantageous to keep the cache window as small as required. The minimum cache window size is therefore dependent upon the diameter of the network. It will be made a configurable parameter.

6.4 Multi-channel Support

As previously mentioned the overlying architecture of a MV-BPL network is based on segmenting the overall MV network into multiple MV-BPL cells where each cell has a connection at one gateway SS to the WAN (see Figure 27). In order to avoid neighboring cells from interfering with each other, it is necessary to have neighboring cells operate on orthogonal frequency channels according to a Frequency Division Multiplexing (FDM) architecture. The available spectrum is allocated to different PLC networks and each network operates in a part of the available spectrum. Each MV-BPL cell could then operate concurrently and asynchronously (and therefore inherently independently).

An FDM architecture with PLC presents a significant challenge due to the very high dynamic range of the PLC system. It is fairly common that signals received from PLC nodes located very close to the receiver are very strong compared to signals that are received from PLC nodes that are located further away from the receiver. This is due to the fact that the attenuation will increase - and for some wiring rather significantly - with distance. This attenuation is not only due to physical effects of the wiring (e.g. dielectric losses), but also due to the increased number of branches which lead to attenuation due to multipath effects. Therefore, a receiver must be able to receive very weak signals as well as very strong signals with a required dynamic range as high as 80 dB in some cases.

The main component providing the realization of this dynamic range is the Analog Front End (AFE). The AFE provides analog/digital signal conversion, filtering, Variable Gain Amplification (VGA) and switching (between receive/transmit) functionality with analog hardware. The transmit chain of the AFE must be able to provide a high current in order to provide sufficient power for complex impedance conditions. The functionality of the receive chain is more complex. The receive chain will typically consist of analog filters, a low noise amplifier (LNA) and a VGA followed by the analog to digital converter (ADC). The main goal of the receive chain is to adjust the amplitude of the incoming analog signal in order to maximize the resolution provided by the ADC. This means that the amplitude of the incoming signal must be adjusted such that it is high enough, but not too high as that would lead to clipping/distortion of the incoming signal. If the incoming analog signal purely consists of the desired communications signal, then this functionality is rather straightforward. However, as noise and interference is introduced to the communications signal the task becomes more complex. If the noise/interference is out-of-band (outside the communications signal spectrum) then it can potentially be filtered before entering the ADC. However, if the noise/interference is in-band (within the communications signal spectrum) then the receive chain must adjust the gain such that the noise/interference plus communications signal is within a suitable range of the ADC. For PLUS-Avionics due to the fact that EMC susceptibility testing for avionics applications requires that the system tolerate high frequency High Intensity Radiated Fields (HIRF) this is no trivial task. Out-of-band, but also in-band interfering signals during testing may be as high as several volts whereas the PLC signal may be within the millivolt range. In extreme cases pulsed spikes caused by relay switching can be as high as 20 volts in-band. This often requires extensive attenuation of the signal in order to make sure that the amplitude is within the range of the ADC.

Over 10 years’ experience of Iberdrola has gone into the evaluation of optimum channels to use for MV-BPL with the result being the following three channels [28]:

A. 2-7 MHz

B. 8-18 MHz

C. 20-30 MHz (limited to cables with a shorter length, e.g. <300 m)

In principle the OFDM technology used in the Physical Layer of PLUS would allow these channels to be realized through the use of a tone mask. In other words all OFDM sub-carriers (tones) would be disabled except for the sub-carriers within the targeted frequency ranges. However, performance of OFDM systems tends to suffer as a large portion of the available sub-carriers are disabled. For example, for channel A (2-7 MHz) almost 90% of the sub-carriers would have to be disabled.

Nevertheless, in an independent project partially supported by the Swiss Federal Office of Civil Aviation (FOCA) a multi-channel solution has been developed [29]. Although this solution has been targeted for the avionics domain, it can also be used for the PLUS-Smart Grid solution. The developed PLUS-Multi-Channel solution provides five different FDM modes as shown in Table 5. This table also shows how the different channels will influence the latency and the PHY data rates. The OFDM symbol duration shows the length of a single OFDM payload symbol. The longer this is, the longer the latency of transmitting a PHY Protocol Data Unit (PPDU) on the channel will be. The maximum PHY data rate shows the data rate assuming that all active tones are modulated with the highest modulation (1024-QAM). Again, this is another example of the design trade-off shown in Figure 11. Supporting more channels will improve the network size criteria, but at the cost of higher latency and reduced throughput. The following mapping is considered for supporting the channels identified by Iberdrola as optimal for MV-BPL:

- Channel A → Mode E with center frequency 3.5 MHz
- Channel B → Mode D with center frequency 13 MHz
- Channel C → Mode D with center frequency 25 MHz

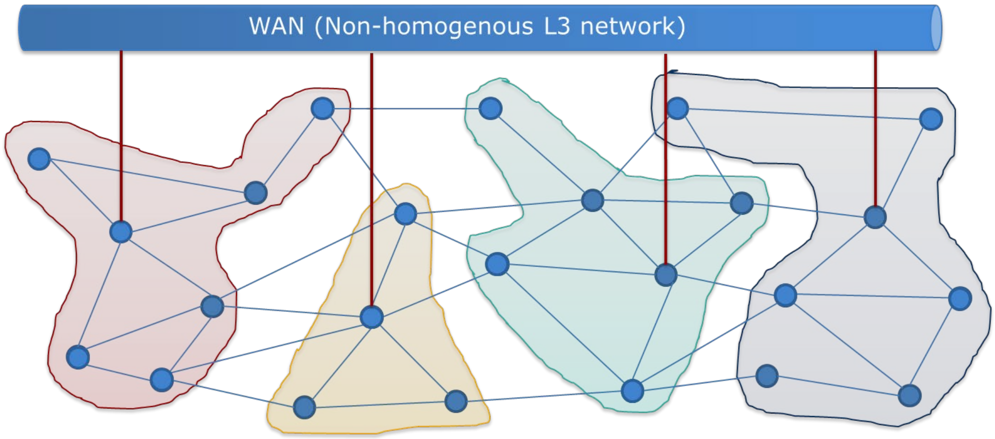


Figure 27: MV-BPL Network Architecture with Multiple Cells

Mode	Number Active Tones	Sampling Frequency	Tone Spacing	Channel Bandwidth	OFDM Symbol Duration	Maximum PHY Data Rate
A	1641	100 MHz	24.41 kHz	40 MHz	40.96 µs	142.44 Mbps
B	1793	100 MHz	16.28 kHz	30 MHz	61.44 µs	103.76 Mbps
C	1641	100 MHz	12.21 kHz	20 MHz	81.92 µs	71.22 Mbps
D	1641	100 MHz	6.10 kHz	10 MHz	163.84 µs	35.61 Mbps
E	1641	100 MHz	3.05 kHz	5 MHz	327.68 µs	17.80 Mbps

Table 5: PLUS-MultiChannel Specification

6.5 Interface to Smart Grid Application Devices

Figure 28 shows the general network protocol stack of the PLUS modem as well as the interfacing to the Smart Grid application devices (called Smart Grid Device in the following). The protocol stack on the Smart Grid Device currently shows the most common protocols IEC 61850 and IEEE C37.118.1. It is assumed that these protocols work on top of a TCP/IP/Ethernet protocol stack and therefore the data interface to the PLUS modem will be Ethernet-based. Although only one application device is shown the potential exists to interface the PLUS modem to several application devices through a Local Area Network (LAN) within the SS. In addition to the Ethernet data interface a second interface is available for providing the time-synchronization to the Smart Grid Device. The time synchronization is provided based on a one pulse per second (1PPS) signal which is a widely accepted standard for time-synchronization. The PLUS modem will consist of the standard PLUS protocol stack (PLUS PHY and PLUS DLL – see also Figure 6) as well as the additional modules for Ethernet gateway functionality (EDS), time synchronization (PLUS-TimeSync) and routing (PLUS_ROUTE). At the other side the PLC interface on the PLUS modem would interface to the coupler hardware (see Figure 7).

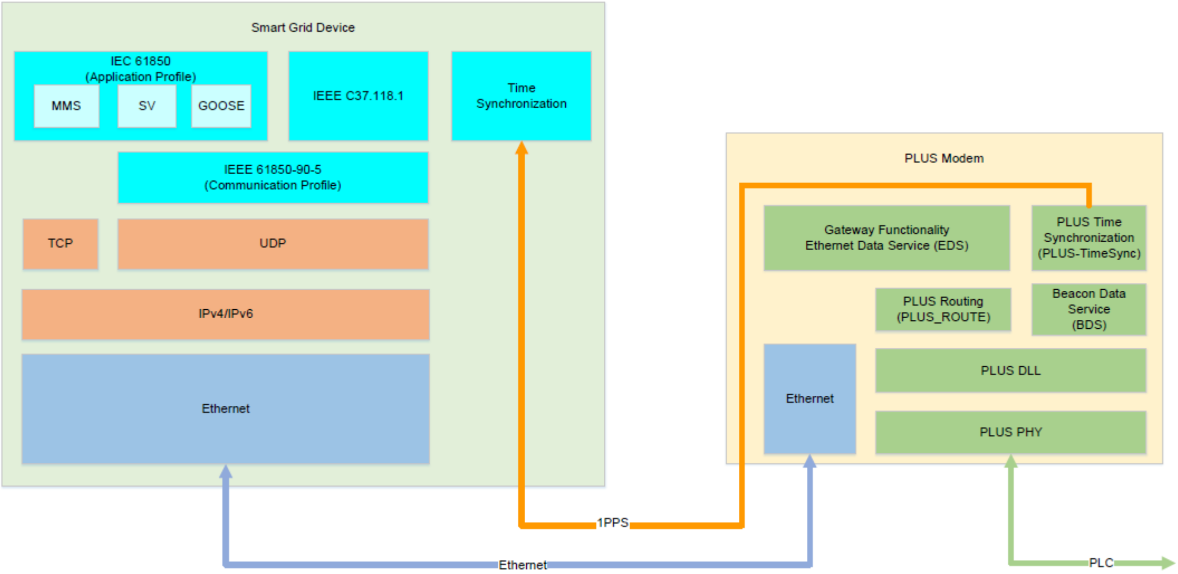


Figure 28: PLUS Network Protocol Stack and Interface to Smart Grid Device

7 Development Process Optimization

One critical part of developing a technology for MTC applications is fulfilling the relevant Design Assurance Guidelines (DAG) for each environment in which the technology is used. A DAG provides guidelines for development processes to ensure that no additional errors have been introduced during the development. It typically includes the definition of different levels of requirements, coding guidelines, review and extensive testing. As the PLUS technology has been designed to be used in MTC applications HSLU has defined a development process from the earliest stages of the development of PLUS. State-of-the-art methodologies like Model Based Design (MBD) are at the core of this process.

The design and verification and validation (V&V) process for PLUS PHY have been defined based on concepts from RTCA DO-254 [23] and RTCA DO-331 [24] and are shown in Figure 29. More details can be found in [22]. The capture of textual hardware requirements serves as the beginning to the design process just as with a standard design (not based on MBD). However, the hardware design process is based around two different levels of models, a conceptual design model and a detailed design model.

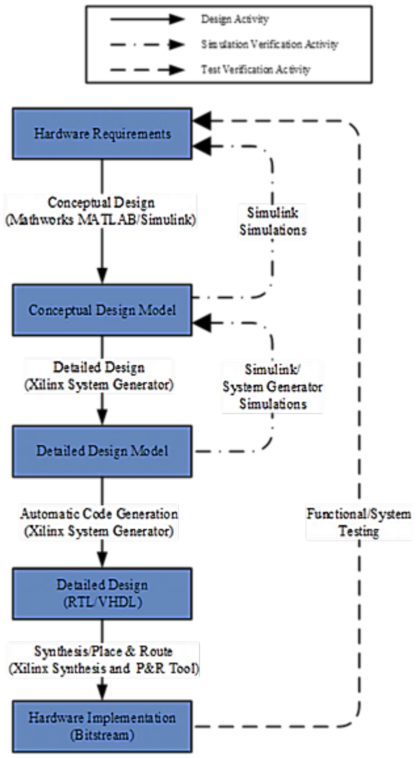

Design Activity
Simulation Verification Activity
Test Verification Activity
Hardware Requirements
Conceptual Design (Mathworks MATLAB/Simulink)
Simulink Simulations
Conceptual Design Model
Detailed Design (Xilinx System Generator)
Simulink/ System Generator Simulations
Detailed Design Model
Automatic Code Generation (Xilinx System Generator)
Functional/System Testing
Detailed Design (RTL/VHDL)
Synthesis/Place & Route (Xilinx Synthesis and P&R Tool)
Hardware Implementation (Bitstream)

Figure 29: PLUS PHY Design and V&V Process Overview

MBD is used both within the conceptual and detailed design with high-level MATLAB based models provided for the conceptual design and low-level detailed design models using Xilinx System Generator. Simulation of the executable models is used in order to provide an initial verification of the conceptual design models against the hardware requirements and to verify that the behavior of the detailed design models is the same as the conceptual design models. MBD has been found to provide a number of advantages including

- Complex design may be more easily broken down into manageable design tasks
- Issues may be identified at an earlier stage in the design process
- A shorter iteration time with less effort is required to solve issues or provide optimizations
- Various design aspects may be investigated and tested in a controlled and reproducible environment
- The influence of important aspects under investigation may be isolated from other factors and quantitatively evaluated.

Both the conceptual design model and detailed design model are executable, meaning that simulations may be used in order to provide an initial two-step verification of the design against the textual requirements before functional testing of the implementation on the hardware platform.

Within this project a new concept for extending V&V testing has been developed which is shown in Figure 30. This new process can be considered as Hardware-in-the-Loop (HIL) testing. In essence this process closes the loop of the MBD approach by allowing captured data samples from hardware testing to be used within specification and design model simulations. The main advantage is that real-world effects from the PLC channel, coupler, Analog Front End (AFE) can be evaluated within a controlled simulation environment. Central to this concept is the use of the Xilinx Integrated Logic Analyzer (ILA). The ILA IP core provides a logical analyser with which selected internal signals from the PLUS modem can be captured during real-time operation. Since these signals must be stored within Block-RAMs within the FPGA, the number of signals and time that each signal can be captured is limited. However, with careful selection of the critical signals and the use of intelligent triggering conditions, sufficient data can be captured. The main signal of interest is the digitized received PLC signal which can be observed at different locations of the PLUS PHY receive chain (see Figure 14). The captured and exported samples of this signal can then be used as an input within simulations. Within simulations the behaviour can be observed in a more controlled environment allowing any possible issues to be better isolated and resolved.

The basic process is the following:

1. Identify the targeted signals and timeframe to be recorded.
2. Introduce and configure the ILA within the design model.
3. Generate a new bitsteam and firmware image with the ILA.
4. Deploy the image to the modems/environment under test.
5. Configure the triggering condition on the modem under test.
6. Capture the signals with the ILA and export to simulation environment.
7. Configure the captured signals as input to either a specification or design model simulation.
8. Simulate and test.

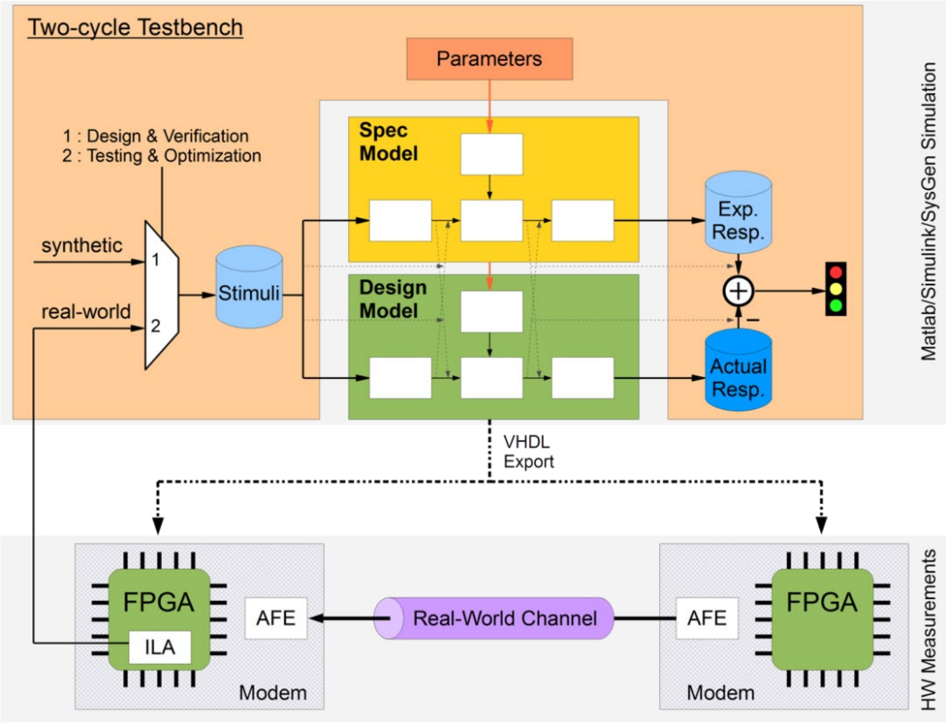


Figure 30: PLUS Hardware-in-the-Loop Test Process

8 MV-BPL Security Analysis

8.1 Introduction

One of the major issues in any telecommunication system is security. For shared media/channels such as the power line channel, this is even a bigger issue. However, when compared to wireless systems, a PLC system at the Medium Voltage (MV) level is by nature more secure because the physical medium of the power line channel – the cabling - is typically not easily accessible. The high voltage levels necessitate a physical separation between the cable/wire and any other objects in order to ensure safety against electrocution. This includes both underground (buried) cable and overhead wires. However, when compared to traditional wired LANs where the stations in the network are closely controlled, power line systems are vulnerable to several attacks. The following attacks can happen on power line systems [15]:

- Attacks for damaging the available working power line network
- Attack to prevent the system operation
- Attack that aims to access to the devices connected to the network.

However, it is possible to overcome these attacks by using several techniques which include:

- Authentication
- Encryption
- Integrity control
- Protection against replay attacks
- Access control
- Anti-jamming techniques

All these different techniques are explained in the following sub-chapters in the general context of PLC over MV lines. Wherever it is relevant, IEEE 1901-based implementation in PLUS is explained.

8.2 Authentication

Authentication is one of the possible software security approaches that can be used in PLC systems as well as any other wired/wireless systems. This security approach authorizes a device to access to the network only after identifying the device [15]. This identification can be done in several ways: Using a unique Device Access Key (DAK), using a pass phrase or identifying a device manually.

An IEEE 1901 standard conform PLC network [9] uses a valid Network Management Key (NMK) to verify if a device is successfully authenticated or not. A device can possess this NMK in different ways [16]:

- Preloaded NMK
  - Devices are sometimes preloaded with the NMK to connect to a network
- Direct Entry of the NMK
  - Directly entering the NMK into the device to connect to a specific network
- Distribution of NMK using a DAK
  - The device gets authenticated with its DAK and gets the NMK encrypted with its DAK

- Distribution of NMK using Unicast Key Exchange (UKE)
    - A user triggers manually an unauthenticated and authenticated device to transfer NMK from authenticated device to unauthenticated device using UKE method
- Distribution of NMK using other key management protocols
    - In addition to the above methods, it is also possible to distribute the NMK using standards like 802.1x, Extensible Authentication Protocol (EAP) and Simple Network Management Protocol (SNMP)

8.3 Encryption

Similar to wireless communications, PLC is intrinsically broadcast, thus the channel is shared between the users in the network. In this scenario, the secrecy plays a crucial role in order to ensure information confidentiality, since, for instance, a transmitter wishes to send confidential information to different users. The secrecy can be provided in two main ways: at the higher OSI layers or at the Physical Layer. The first concerns a cryptographic approach based on algorithms such as the Advanced Encryption Standard (AES) or the RSA. The second exploits the physical medium, its time/frequency diversity and the differences between the users' links in order to provide security. This concept is known as Physical Layer Security (PLS) [17].

PLS is explained for PLC channels in [17] and for wireless channels in [18]. [17] verified that PLS is not feasible for the PLC channel. On the other hand, PLC MAC standards do not provide any specialized security protocol for access control meaning that encryption must be provided. The IEEE 1901 standard uses the 128-bit AES algorithm in counter mode (CTR) for encrypting the data. For the devices based on IEEE 1901, it is mandatory to support both PHY Block-Level Encryption and Payload-Level Encryption [16].

IEEE 1901 specifies different 128-bit AES encryption keys, hash keys (longer, machine-generated strings) for the UKE protocol. Different encryption keys used in IEEE 1901 are listed below:

- Device Access Key (DAK): This is unique to a device and is provided by the manufacture. Another device, which knows a particular device's DAK can use that DAK to encrypt a message.
- Network Membership Key (NMK): This key is used to prove a device's membership in a PLC network. Different ways of provisioning this key were explained in Chapter 8.2.
- Network Encryption Key (NEK): During normal operation, most messages are encrypted using this key. This is generated by the master of a PLC network and transmitted to all the members after encrypting with NMK.
- Temporary Encryption Key (TEK): This key is used to encrypt the communication between two devices with a temporary private channel. The key is either distributed with receiver's DAK or generated using UKE protocol.

8.4 Data Integrity

For a given system, the following may be considered as errors by the data bus:

- Messages arrive too late: This is related to message latency. Since we can assume to be dealing with hard-real time applications it is necessary to deliver messages within an upper time bound. Messages arriving later than this can be deemed as erroneous.

- Messages are not delivered (availability): Certain conditions lead to a signal not being able to be transmitted or received with bit errors being detected. This means that the message is not properly transmitted and/or received. There are several conditions that can lead to message loss, e.g. channel/noise effects, equipment faults, wire faults, etc.
- Undetected message errors (integrity): A message is received with erroneous information (bit-errors), however these errors are not detected by error detection and the message is marked as valid information.

Of these errors undetected message errors are by far the most critical. Almost all systems will be designed to handle a certain amount of message loss or extended latency. They must be able to handle these errors to a certain extent. However, the system has no way of knowing that the data it has received from the data bus actually contains invalid data. This invalid data will then be handled by the system and can lead to catastrophic events. For this reason the probability of occurrence of undetected errors (PUD) must be extremely low.

Cyclic Redundancy Check (CRC) is considered the state-of-the-art in error detection for modern communications systems [21]. Error detection effectiveness depends upon multiple factors including: the size of data to be protected, types of data errors expected, the smallest number of bit errors that are undetectable by the error code (the Hamming Distance), and the undetected error fraction of errors as a function of number of bit errors present in a particular piece of data. CRCs give dramatically better error detection performance than checksums at short to medium dataword lengths due to a higher Hamming Distance (HD) in many cases, and give somewhat better performance even for very long dataword lengths. Not all CRCs are created equal. In fact there are far better CRCs available than the IEEE 802.3 CRC-32 which provide an improved HD. Using CRCs in applications requires attention to numerous other factors including:

- The corruption of header length fields which can lead to looking for the CRC in the frame at the incorrect location.
- Protection of segmented data blocks.
- Interactions between physical layer encoding and CRC[9].

The PLUS Avionics design has taken this into consideration from the very beginning. A multi-level approach has been adopted as shown in Figure 31. The PLUS Avionics error detection scheme provides the following characteristics:

- Extremely long 40-bit CRC protects the Frame Control (FC) header as this header is necessary for decoding the MPDU payload. This ensures that invalid information from the FC is not used which could undermine further error detection.
- Each coded physical block is protected by a 32-bit CRC.
- As the MSDU header contains a length field, it is protected by a 8-bit CRC at a fixed position within the header.
- The overall MSDU is protected by a 32-bit CRC. The MSDU CRC is used to ensure that any errors that might be introduced through segmenting/re-combining the MSDU into physical blocks will be correctly detected so that the internal segmenting/re-combining cannot lead to undected errors.
- Highly effective CRCs have been selected at all levels.

[9] Example: Bit stuff corruption in the Controller Area Network (CAN) undermines the error detection effectiveness.

It is this error detection concept that allows PLUS Avionics to achieve an extremely low PUD). It can be shown through analysis that a PUD < 10^{-13} can be achieved even under extreme channel conditions which could lead to high frame errors (low availability).

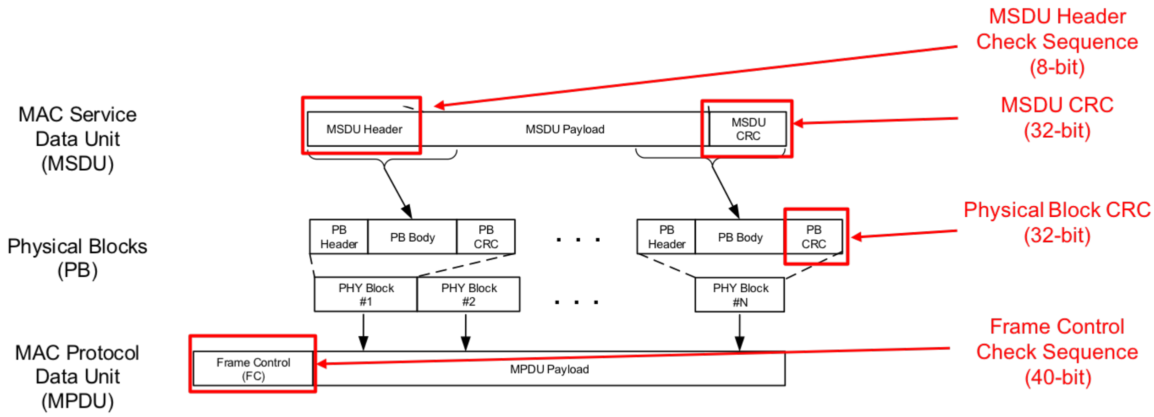


Figure 31: PLUS Error Detection Overview

However, the CRC is not enough in order to ensure that the received message is from the intended sender and that the message was not modified in between the sender and receiver. In the Symmetric key setting or AES, a Message Authentication Code (MAC) is used to ensure the data integrity. This code is generated by the sender with the symmetric key known by the receiver and the receiver verifies the code with the same key and the received message.

IEEE 1901 specifies the usage of Cipher Block Chaining Message Authentication Code (CBC-MAC) in order to ensure the data integrity [9]. The process of obtaining the authentication code is shown in Figure 32 where m is the message, k is the symmetric key and E is the block cipher.

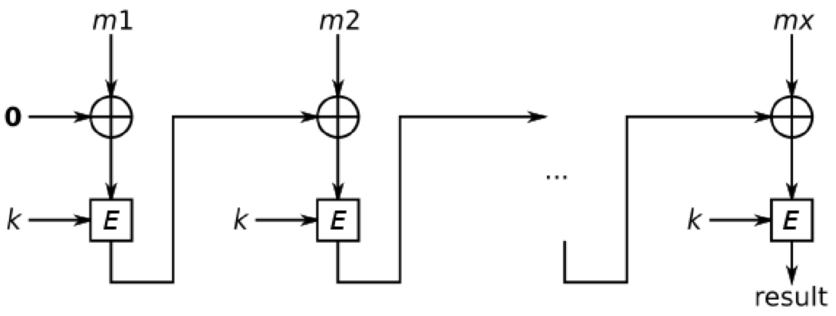


Figure 32: CBC-MAC

8.5 Protection Against Replay Attacks

A replay attack is a form of network attack in which a valid data transmission is fraudulently or maliciously repeated or delayed. These replay attacks can be prevented by using session IDs, one-time passwords, nonces, and timestamps. IEEE 1901 uses nonces, which are pseudo-random numbers that are used only once. Since the number of bits in a nonce is finite, there is a possibility of a repetition. However, same nonces are avoided while using the same encryption key [16].

8.6 Physical Access Control

In order to ensure the security for MV-BPL, it is necessary to verify the physical security of the communication medium and the PLC modems, which are in operation. In the case of MV-BPL, MV lines are acting as the communication medium and the PLC modems are located in the SSs.

MV transmission lines have nominally voltages between 1 kV and 35 kV. They are used to connect the primary substations that terminate the HV transmission network to the SSs. Within the SSs transformers generate and distribute the LV network. The transmission lines are either underground cables or overhead wires. Typically, European countries tend to have a high proportion of underground cables [19]. Physical security of these underground cables and overhead wires are ensured by the presence of high voltage AC electrical signal, as it is very dangerous to access these wires physically.

SSs are at the heart of the MV distribution network. They are typically consisting of switchgear and a step-down transformer. Unauthorized access to these SSs can result in huge financial losses as well as cause power outages. There are many recommendations to the utilities to deploy security measures, which include:

- Video surveillance: Remote monitoring using video cameras.
- Substation access control: Identification, authentication and recording of authorized individuals accessing the facility.
- Perimeter sensors: Fences around a substation can be configured with thermal/motion sensors that detect movement.

8.7 Anti-Jamming Techniques

Typically, jammers are used to disrupt a communication system and there are several jamming attack schemes available. Some of these schemes are more effective and efficient than others. Several such schemes for OFDM-based wireless systems are explained in [20] and are classified into four categories: Barrage Jamming, Noise Jamming, Interference, and Correlated Jamming. The complexity and effectiveness of these different attack schemes have been studied and some mitigation techniques have been proposed in [20]. This study is mainly for OFDM-based wireless systems where the frequency is ranging from 700 MHz to 2.4 GHz. The complexity and effectiveness of these schemes are shown in Table 6.

Even though the study was done for wireless systems, the attack schemes are also relevant for the MV-BPL. However, there are some major differences regarding the complexity and effectiveness of these schemes. Unlike the studied wireless systems, MV-BPL is typically ranging from 1.6 MHz to 30 MHz and the channel is the MV power line. As explained in Chapter 8.6, getting access to both underground and overhead MV power lines and then couple the signals to the power line is very difficult and dangerous. Also, inductive coupling from a distance to the SS or the power line is very difficult as it requires an extra-large antenna to achieve the same kind of effect as e.g. for the wireless systems. In addition, in underground cables the effect of jamming attacks is physically very limited due to the high insulation. Due to the antenna’s bulkiness, it is highly unlikely that the jamming attacks can be conducted unnoticed.

Overall, it requires a substantial effort in order to conduct jamming attacks to disrupt the MV-BPL communication.

Attack	Complexity	Effectiveness
Barrage jamming	Very low	Low
Noise jamming	Low	Low
Interference	Low	Low
Correlated jamming		
- Synchronisation attack	High	High
- Equalization attack	High	High
- Control channel attack	High	High

Table 6: Jamming Attacks for the OFDM-based Wireless System [19]

8.8 Protection Communication Supervision (PCS)

Protection Communication Supervision (PCS) provides a means for detecting disturbances or beakdowns within the BPL communications link and provide an interface for alerting those disturbances to the protection application. This feature is especially critical for the LDP application, so it is able to determine if it can rely on the underlying communications network or if it should react independently (if communications is not available). The PCS for PLUS has been realized through the use of the Beacon Data Service (BDS) – see also Figure 28. The BDS transmits beacons to all neighbouring modems at fixed intervals, e.g. every 500 ms. Each neighbour monitors the received beacons from its neighbours. Knowing the transmission interval and allowing for a certain amount of packet loss the PCS will make the decision whether specific communication links are available or not. This information is currently made available through a software interface within the PLUS modem. This information could be then made available to the application devices over the Ethernet data interface.

8.9 Summary

Security plays a very important role in smart grid. This chapter has presented an overview of the security threats possible with the MV-BPL communication and with possible solutions. The possible security threats with respect to the communication technology can be mitigated using an authentication procedure, strong encryption, integrity control and protection against replay attacks. Security threats with the communication medium can be mitigated by using common encryption techniques as defined within the IEEE 1901 standard. This project has focussed on the analysis of necessary security measures. As such this encryption has not yet been implemented in the PLUS prototypes. The implementation is rather straightforward and is foreseen for the near future.

9 PLUS-Smart Grid Prototypes

A PLUS modem consists of a number of hardware components as shown in Figure 33.

- PLUS Avionics Protocol DSP: Typically an ASIC or FPGA in which the PLUS Avionics protocol and DSP is realized.
- Analog Front End (AFE): Provides all the analog processing of the PLUS Avionics signal which includes:
  - Digital-to-Analog Converter (DAC)
  - Analog-to-Digital Converter (ADC)
  - Variable Gain Amplifier (VGA)
  - Line Driver
  - Switching between the receiver and transmit chains
- PLC Coupler: Responsible for superimposing the high-power, low-frequency power signal with the low-power, high-frequency PLC signal. The size of the analog coupler components are determined by the required voltage and current specification.

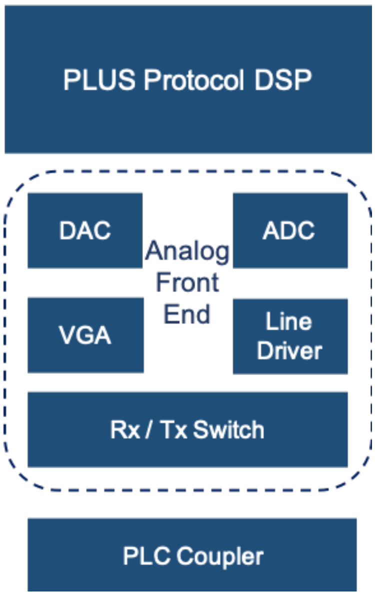


Figure 33: PLUS Modem Architecture

It is critical that the PLUS algorithms can be realized with the limited hardware resources. From the beginning the realization potential of any algorithms has been an important design criteria. No algorithms have been introduced that could not be realized with real-time execution on the target prototype platform. Just as the PLUS protocol has evolved over time as optimizations have been identified, the PLUS prototype hardware platform has evolved over time.

It was known from an early stage that a hardware prototype realization of the PLUS protocol must remain flexible in order to support the different requirements of different application areas. For this reason, the Xilinx Zynq System-on-Chip (SoC) platform was selected as the basis for initial PLUS prototypes. Xilinx Zynq was selected due to the flexibility of providing both an FPGA (Programmable Logic - PL) together with a CPU (Processing System - PS) on a single chip. A high speed AXI bus connects the PS to the PL. In order to provide more flexibility, the higher layers of the PLUS protocol have been realized in software (C-code) which runs on CPU Core 1. The lower layers of the PLUS protocol have been realized within the PL. The partitioning of the PLUS protocol is shown in Figure 35. In addition, a Linux OS is provided which runs on CPU Core 0. This OS is independent of the PLUS protocol functionality and is used in order to aid in remote access, debugging and testing of the PLUS prototypes. Testing within this project as described in Chapter 10 has been carried out on the latest prototype hardware – PLUS Prototype Hardware 3.0 which has been developed in an independent project. A picture of the new modem hardware is shown in Figure 34. The first three versions of the PLUS prototype hardware are based on the Xilinx Zynq SoC. Although highly flexible, the Xilinx Zynq based solution has two distinct disadvantages: 1) it is expensive and 2) it would make the certification extremely challenging. For this reason, an FPGA solution is targeted for the fourth generation PLUS prototype. The parts of the PLUS protocol that have previously been realized within software have now been realized in VHDL. The fourth-generation prototype will therefore provide an all-VHDL solution providing an easier path toward certification based on DAG (see Chapter 7).

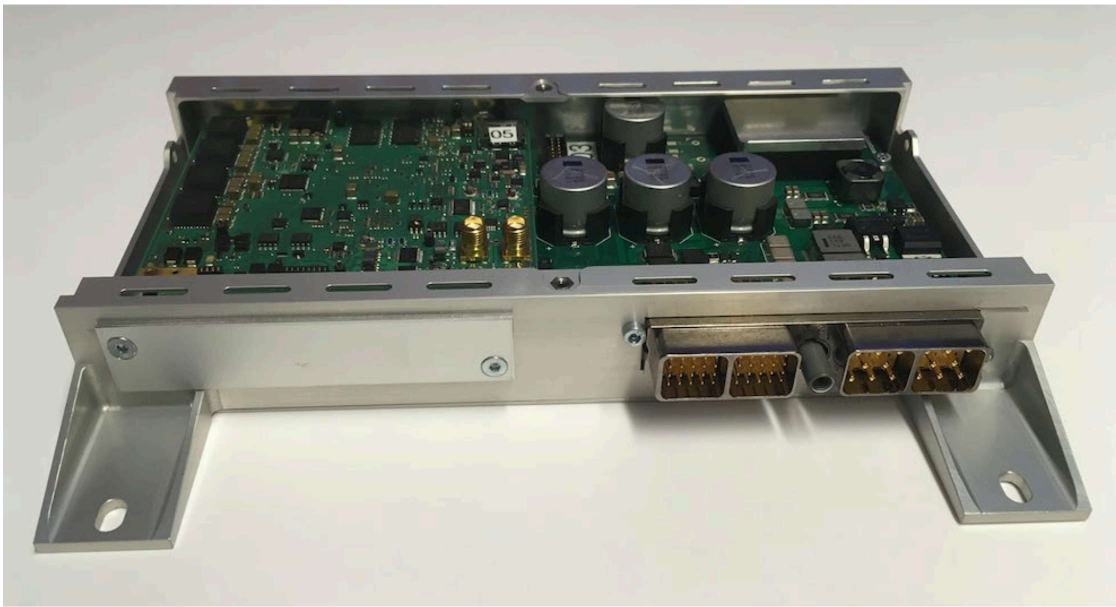


Figure 34: PLUS Prototype Hardware 3.0

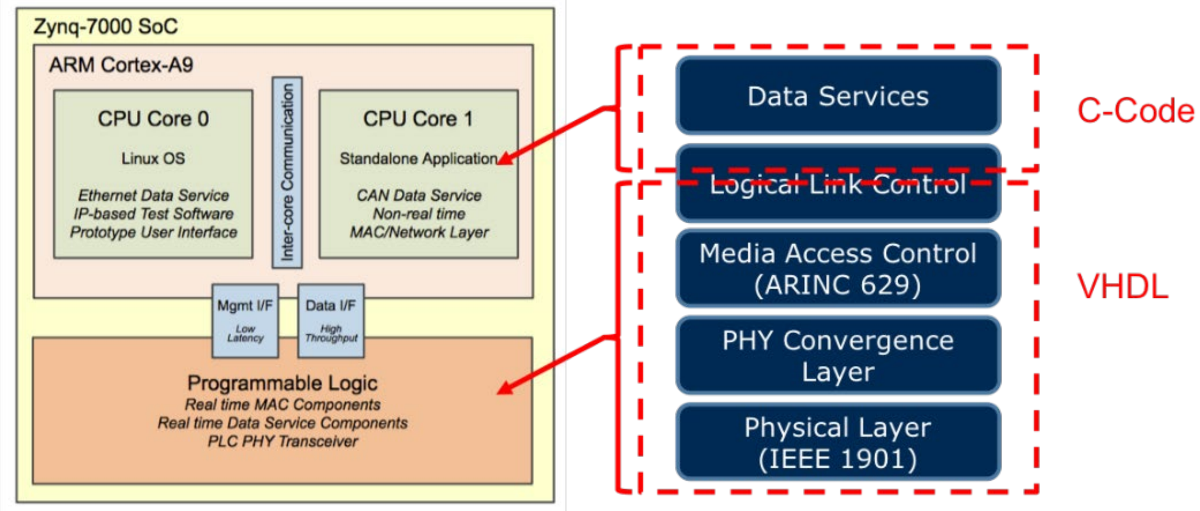


Figure 35: PLUS Prototype Realization Architecture with Xilinx Zynq

Figure 36 shows the high-level architecture of the prototype as it has been realized within this project. Red boxes highlight the areas in which features previously described have been implemented for the realization of the PLUS-SmartGrid solution which includes:

- PLUS-Time Synchronization (PLUS-TimeSync) [see Chapter 3.5]: Realized in VHDL code in Zynq Programmable Logic (PL)
- Beacon Data Service (BDS) [See Chapter 8.8]: The BDS is used to realize a Protection Communication Service (PCS). This is realized in VHDL code in the Zynq PL.

- Data Service Switch (DS_SWITCH) and Logical Link Control Hardware (LLC_HW): In the previous SFOE project in which PLUS-TimeSync has been developed the time synchronization protocol was only partially integrated with the full PLUS protocol. It was implemented such that only the management beacons for the PLUS-TimeSync could be sent, but not any data frames (MPDUs). This was sufficient for demonstrating the performance of the PLUS-TimeSync protocol performance. Within this project PLUS-TimeSync has been cleanly integrated such that management beacons can be sent in parallel with data frames. This has been realized through the implementation of the logical link control and data service switch blocks in VHDL in the Zynq PL. Data services can now be supported both in PL as well as PS.
- PLUS-Routing (PLUS-Route) [See Chapter 6.3]: The PLUS routing protocol has been implemented in C-code in the Zynq Processing System (PS) on CPU1. It has been interfaced to the Ethernet Data Service (EDS) as only EDS is foreseen for use with the PLUS-SmartGrid technology.
- MAC-CSMA [See Chapter 6.2]: Within this project an initial version of the PLUS-TokenRing protocol has been implemented. This includes a CSMA/CA based MAC (MAC-CSMA) as well as a static token passing protocol. Project resources were not sufficient to implement the full PLUS-TokenRing protocol. However, the available static implementation is sufficient in order to perform lab testing with the protocol and verify its basic functionality. PLUS-TokenRing has also been identified to be useful within other potential application areas for PLUS (e.g. as a train communications network). Therefore, the full implementation of a dynamic PLUS-TokenRing protocol has been left for a future project.
- PHY Receiver (RX_PHY) [See Chapter 5.4 and Chapter 5.5]: Parallel decoding as well as higher order modulations have been implemented.
- PHY Transmitter (TX_PHY) [See Chapter 5.3 and Chapter 5.5]: The optimized FFT as well as higher order modulations have been implemented.
- PLUS-Multichannel (PLUS-MC) [See Chapter 6.4]: The PLUS-MC implementation developed in the Swiss FOCA project [29] has been integrated into the PLUS-Smart Grid technology.

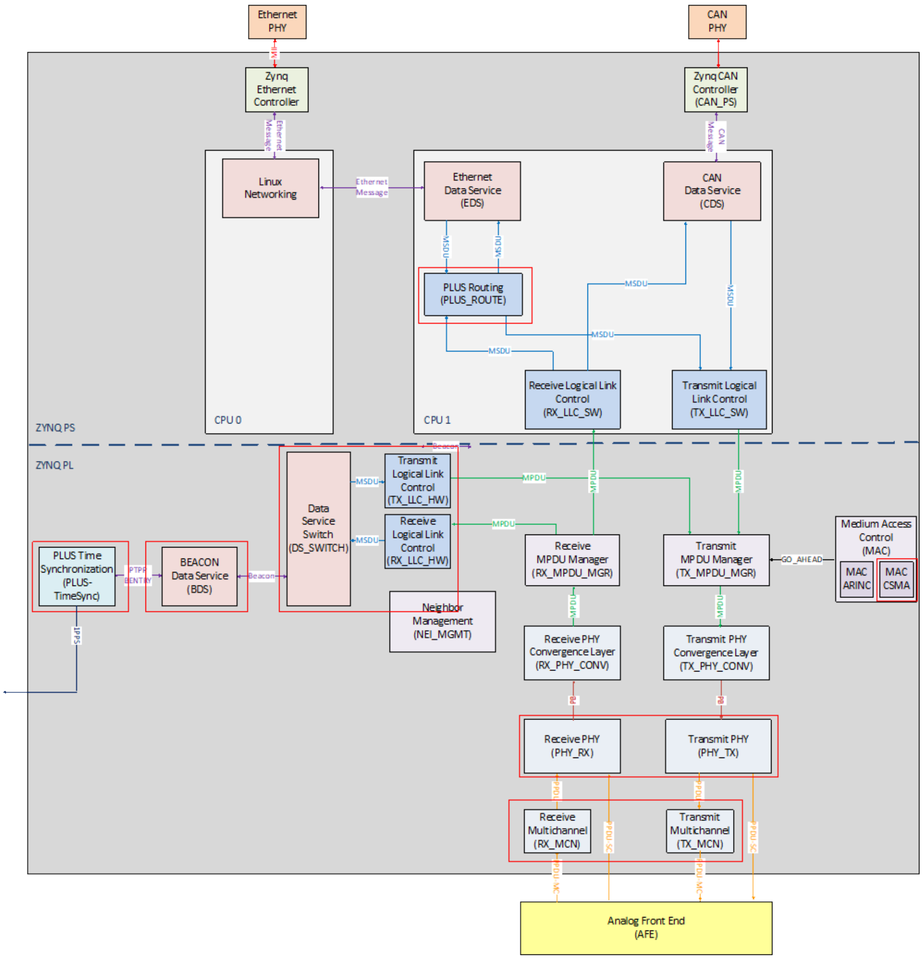

Ethernet PHY
MII
Zynq Ethernet Controller
Ethernet Message
Linux Networking
Ethernet Message
Ethernet Data Service (EDS)
CAN PHY
Zynq CAN Controller (CAN_PS)
CAN Message
CAN Data Service (CDS)
MSDU
MSDU
PLUS Routing (PLUS_ROUTE)
MSDU
MSDU
MSDU
MSDU
Receive Logical Link Control (RX_LLC_SW)
Transmit Logical Link Control (TX_LLC_SW)
CPU 0
CPU 1
ZYNQ PS
ZYNQ PL
Beacon
Data Service Switch (DS_SWITCH)
MSDU
MSDU
Transmit Logical Link Control (TX_LLC_HW)
Receive Logical Link Control (RX_LLC_HW)
MPDU
MPDU
MPDU
MPDU
PLUS Time Synchronization (PLUS-TimeSync)
PTPP BENTRY
BEACON Data Service (BDS)
Beacon
1PPS
Neighbor Management (NEI_MGMT)
Receive MPDU Manager (RX_MPDU_MGR)
Transmit MPDU Manager (TX_MPDU_MGR)
GO_AHEAD
Medium Access Control (MAC)
MAC ARINC
MAC CSMA
MPDU
MPDU
Receive PHY Convergence Layer (RX_PHY_CONV)
Transmit PHY Convergence Layer (TX_PHY_CONV)
PB
PB
Receive PHY (PHY_RX)
Transmit PHY (PHY_TX)
PPDU
PPDU
PPDU-SC
PPDU-SC
Receive Multichannel (RX_MCN)
Transmit Multichannel (TX_MCN)
PPDU-MC
PPDU-MC
Analog Front End (AFE)

Figure 36: PLUS Modem Prototype High-Level Architecture

10 Laboratory Testing

10.1 Introduction

Field testing of MV-BPL solutions is rather expensive due to the high costs of equipment installation within the SSs at the MV level. Safety regulations usually require that the MV-BPL coupler be installed when no voltage is present on the MV line.

Therefore, testing has been performed on three different laboratory test setups as will be described in the following sub-chapters. More extensive field trial testing of the developed solution on a real MV grid will be performed within a follow-up SFOE Pilot+Demo project (see Chapter 11). A brief description of the different test setups as well as a description of some of the test results are provided in this chapter.

10.2 Test Setup A – HSLU/BKW Smart Grid Laboratory

As previously mentioned, the developed PLUS-Smart Grid technology has been tested for potential use as a communication technology for Energie Pool’s iCommUnit product (see Chapter 2.2). The general system architecture for the iCommUnit is shown in Figure 37. The iCommUnit serves as a gateway between Energie Pool's AMI Cloud and one or more smart meters. The iCommUnit is installed within a home, multi-dwelling unit or large industry building. It connects to the smart meters using narrowband G3-PLC technology over the building's power network. Until now the only interfaces to the cloud through the WAN have been mobile technology (2G/3G/4G) and Ethernet (to connect to a home router). As shown in Figure 37 this has been extended to support BPL as an interface.

These three potential communications interfaces between the iCommUnit and the cloud have been tested within the HSLU/BKW Smart Grid Laboratory which is shown in Figure 38. Long term measurements were performed. The measurement values or objects as shown in Table 8 were read at one-minute intervals for each interface over a two-week period. Figure 39 shows an example of different values read over a 24h interval. The average time required to read out each measurement has been analysed and are shown in Table 7.

	Average Measurement Reading Time
Ethernet Connection	6.4 seconds
Cellular Connection	7.2 seconds
MV-BPL	6.4 seconds

Table 7: Smart Meter Reading Performance Results

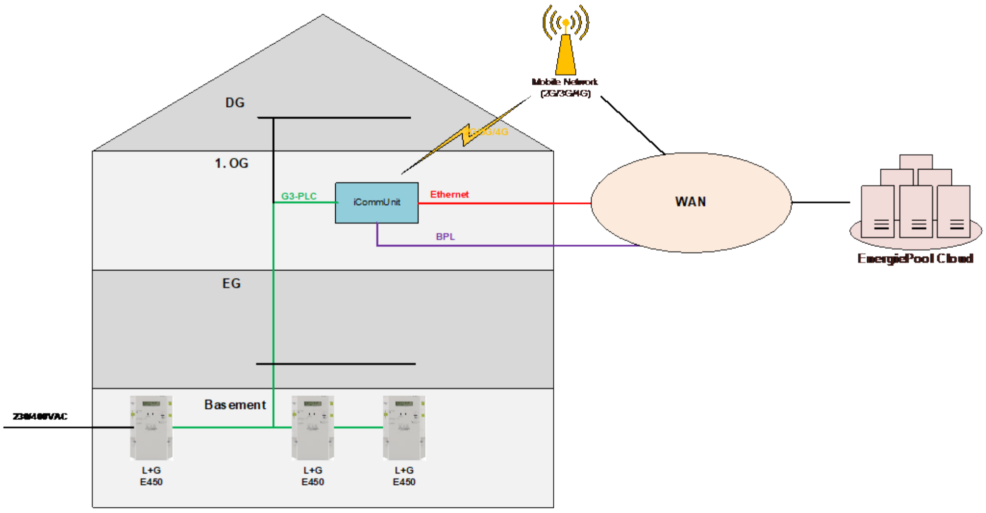


Figure 37: iCommUnit System Architecture

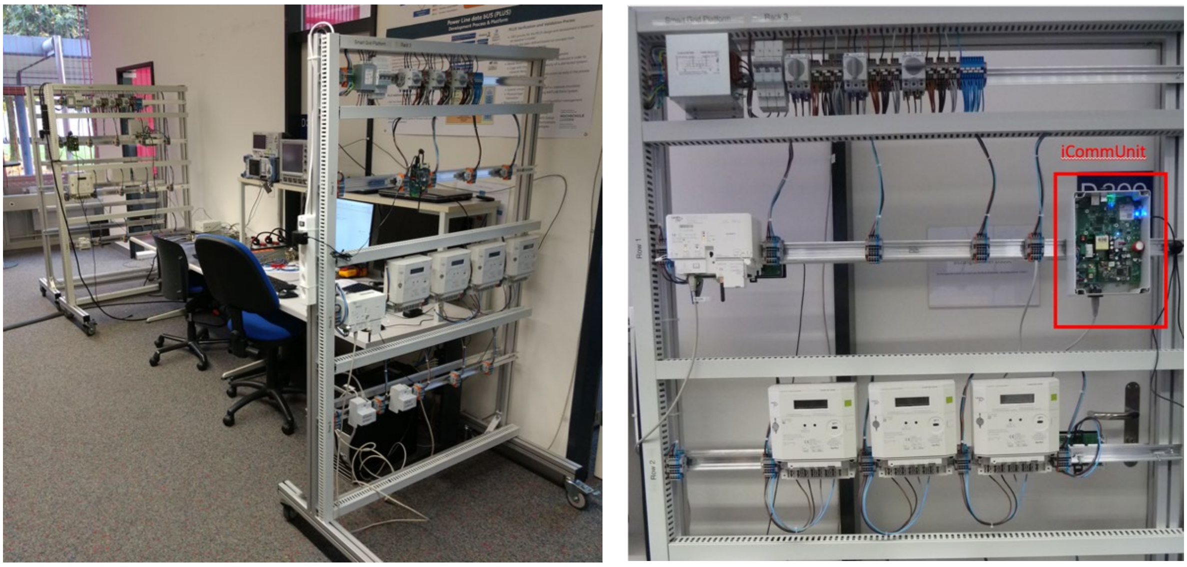


Figure 38: Test Setup B - HSLU/BKW Smart Grid Laboratory

IDIS	OBIS code	Class_id	Attributes to read
Average Voltage L1	1.0.32.24.0.255	3	2
Average Voltage L2	1.0.52.24.0.255	3	2
Average Voltage L3	1.0.72.24.0.255	3	2
Sliding Average current L1	1.0.31.4.0.255	5	2
Sliding Average current L2	1.0.51.4.0.255	5	2
Sliding Average current L3	1.0.71.4.0.255	5	2
Magnitude of last voltage sag in phase L1	1.0.32.34.0.255	3	2
Magnitude of last voltage sag in phase L2	1.0.52.34.0.255	3	2
Magnitude of last voltage sag in phase L3	1.0.72.34.0.255	3	2
Instantaneous active import power (+A)	1.0.1.7.0.255	3	2
Instantaneous active export power (-A)	1.0.2.7.0.255	3	2
Instantaneous reactive import power (+R)	1.0.3.7.0.255	3	2
Instantaneous reactive export power (-R)	1.0.4.7.0.255	3	2
Average Total Power (|+A|+|-A|)	1.0.15.24.0.255	5	2
Average Net Power (|+A|-|-A|)	1.0.16.24.0.255	5	2

Table 8: Smart Meter Measurement Objects

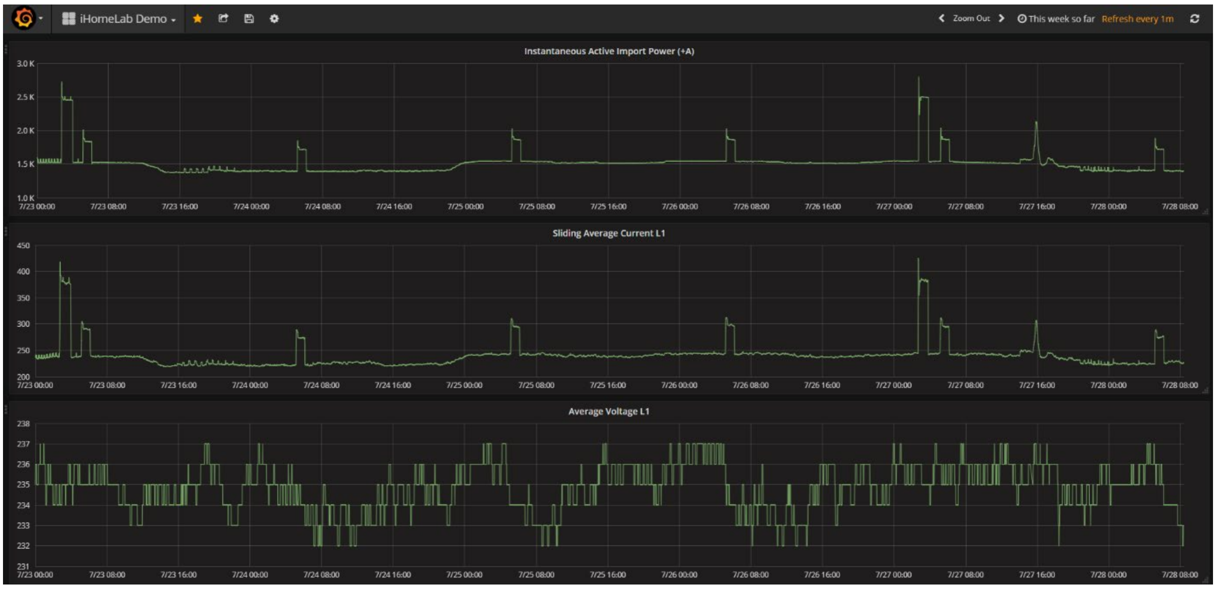


Figure 39: Example Smart Meter Readings over Time

10.3 Test Setup B – HSLU BPL Test Laboratory

HSLU possesses a BPL laboratory test environment which can be considered highly representative of the true MV environment. Extensive models for the transmission channel both on underground cables as well as overhead wires have been developed in previous Swiss CTI projects based on measurements in real MV environments [34]. These models are not only reproduced in the simulation environments previously described but can also be reproduced to a certain extent in the laboratory environment using channel emulators. The test setup used for testing the MV-BPL solution is shown in Figure 40. It consists of a cluster of three MV-BPL modems. PLC Modem A acts as the cluster master. PLC Modem B connects directly to the cluster master, i.e. PLC Modem A. PLC Modem C connects to PLC Modem B. Therefore, PLC Modem B acts as a repeater modem between A and C. In other words, a connection over two hops in the network can be tested. The BPL channel emulator is able to reproduce attenuation and noise conditions which are representative of a MV-BPL network. In the indoor lab environment, a reliable GPS signal is not available. Therefore, the GPS clock or the absolute time is emulated by a simple function generator which is used to output a 1PPS signal. This signal is split and additionally input to the oscilloscope for comparing the time at the modems to the absolute time. The output reference time from each modem provided to the end devices through the 1PPS signal is used for measurement purposes. Within the test setup this time reference from all three modems is input to an oscilloscope such that any differences can be accurately measured.

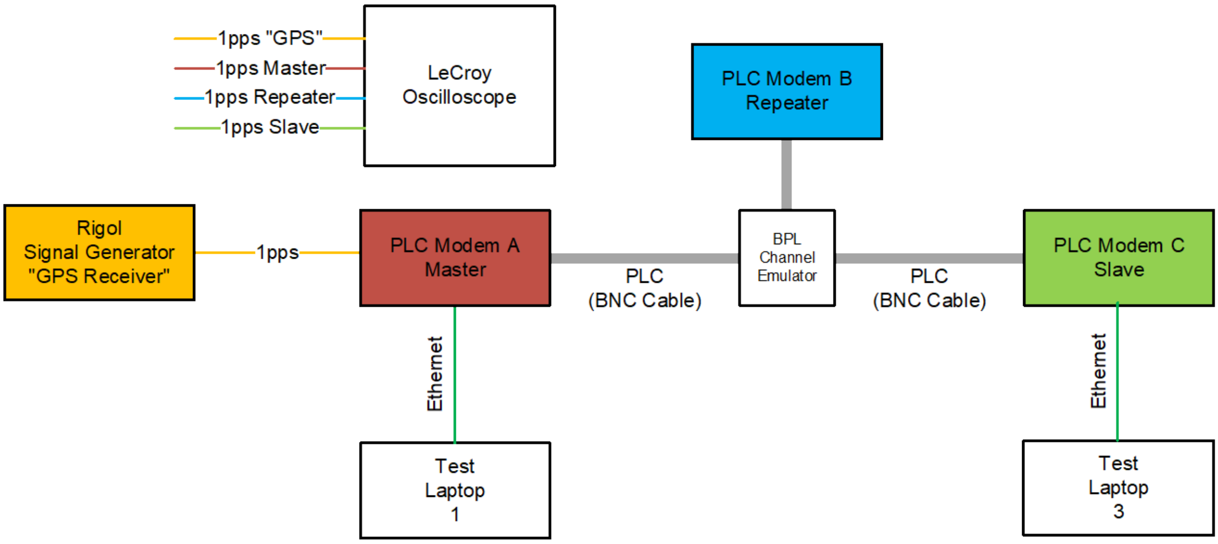


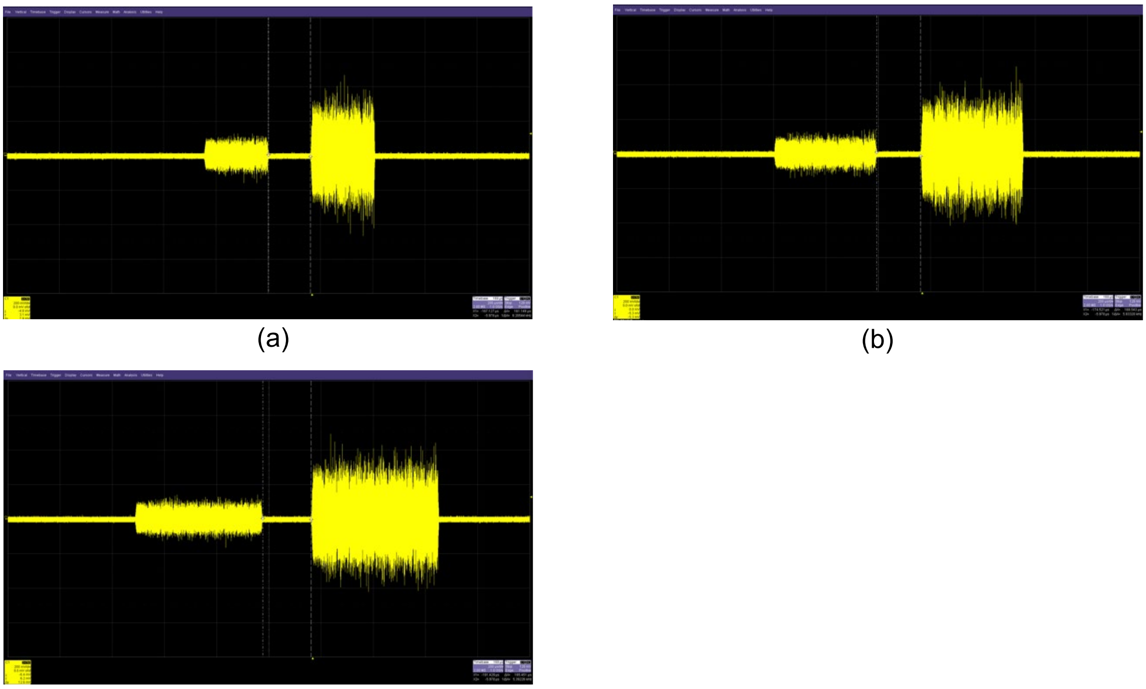
Figure 40: Test Setup B - HSLU BPL Test Environment

This test setup was used in order to verify the latency which has been introduced due to the repeater functionality which has been described in Chapter 6. This will also inherently include the optimizations which have been performed in terms of receive and transmit processing delay. This is due to the fact that when repeating is performed the PLC frame must be fully decoded on the receive side and then fully encoded on the transmission side.

The length of the payload message will also have an influence on the transmission’s duration according to the framing concept shown in Figure 22. Longer frames will also require more time for encoding and decoding. Therefore, it is to be expected that the longer the frame, the higher the latency. The long MPDU size of 1’500 bytes represents the maximum typical Ethernet MTU size and is therefore expected to be the maximum frame size that must be supported for transmission over the PLC network. For testing purposes three different payload message lengths have been defined:

- Short MPDU: Payload messages up to 150 bytes
- Medium MPDU: Payload messages up to 500 bytes
- Long MPDU: Payload messages up to 1’500 bytes

The latency introduced due to repeating has been measured in the test setup using an oscilloscope. Modem A transmitted a frame which was forwarded by modem B to modem C. Therefore, on each “hop” when repeaters are used the frame duration as well as the repeating delay will contribute to the overall end to end latency. Example measurements are shown in Figure 41 for the different MPDU sizes. The OFDM PLC signal for the MPDU transmitted from modem A to modem B can be seen on the left of those measurements. The OFDM PLC signal on the right represents the MPDU transmitted from modem B to modem C. The measured interval between these two PLC signals represents the repeating delay at modem B. These measurements have been repeated for different channel conditions in the test environment. Figure 42 has integrated the results showing how the latency will increase versus the number of repeaters. From Table 1 we know that the maximum latency requirements for the LDP application is 5 ms and for the PMU application 20 ms. From these results we can then gain the maximum number of repeaters that can be supported while still fulfilling the application latency requirements which is shown in Table 9.


(a)

(b)

(c)

Figure 41: Repeater latency testing – (a) short MPDU, (b) medium MPDU, (c) long MPDU

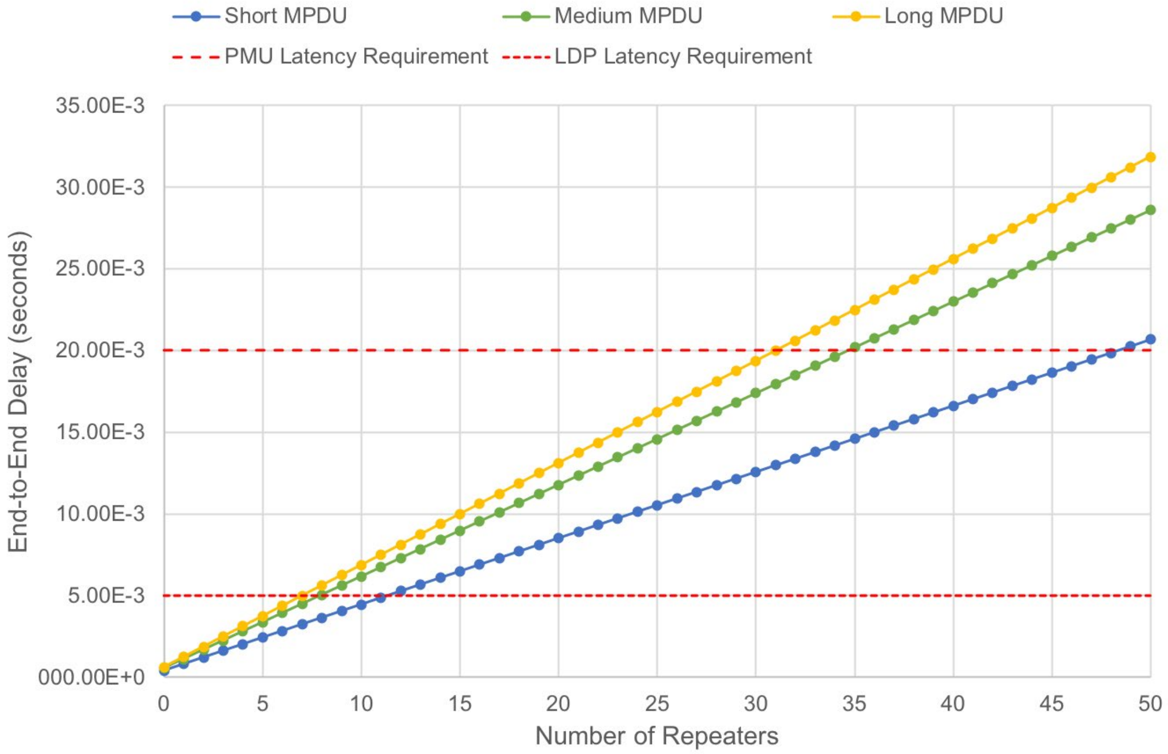


Figure 42: Repeater latency results

	LDP	PMU
Short MPDU	11	48
Medium MPDU	8	35
Long MPDU	7	31

Table 9: Maximum Number of Supported Repeaters

10.4 Test Setup C - HSLU Medium Voltage Overhead Testbed

HSLU has adapted an available MV overhead test line at their facilities in Horw in order to perform BPL testing. This line is not an energized MV line but has been installed with representative wiring and construction. An important factor is that this line will be representative in terms of the noise that is coupled onto the line from external sources, e.g. broadcast radio. For this reason, “long-term” tests with different modulations have been performed on the overhead testbed in order to measure the reliability of the transmission. For different modulations a test has been made over 75 hours. During this period a measurement was made every minute of the Signal-to-Noise-Ratio (SNR) as reported by the modem plus the physical layer (PHY) throughput. Variations in throughput are due to bit errors occurring, e.g. due to noise. Some measurements are shown in Figure 44, Figure 45 and Figure 46. As can be seen the SNR will vary over time which is expected due to the time-variant nature of the noise. This causes a slight variation in the achievable throughput; however no major variations are seen (throughput decreasing dramatically towards zero).

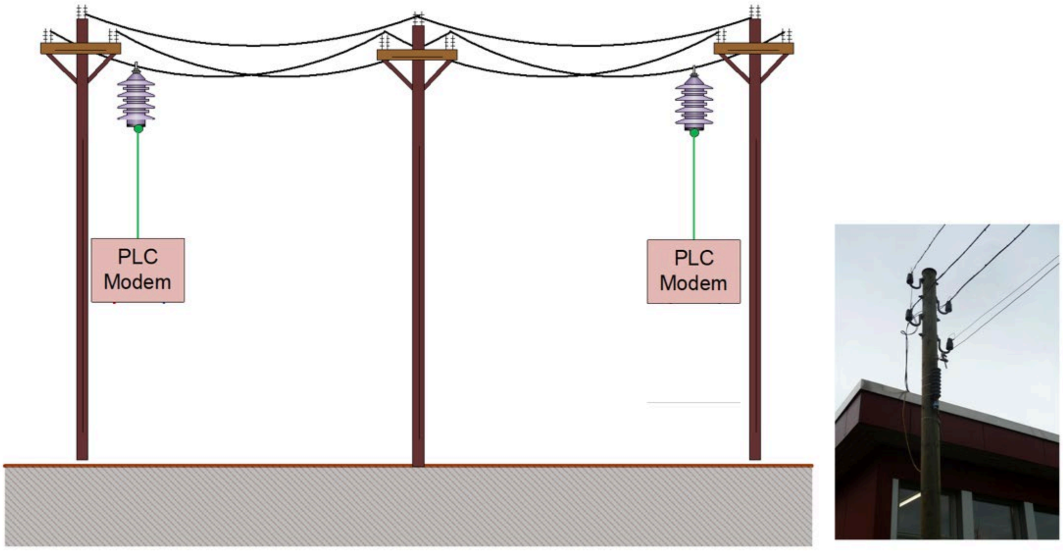


Figure 43: Test Setup C - Medium Voltage Overhead Testbed

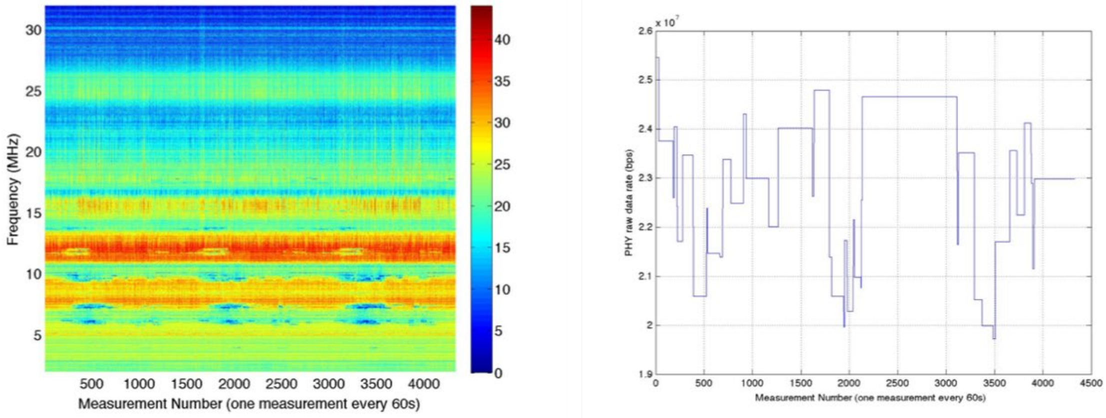


Figure 44: Long term SNR (left) and PHY data rate (right) with nominal data rate of 24 Mbps

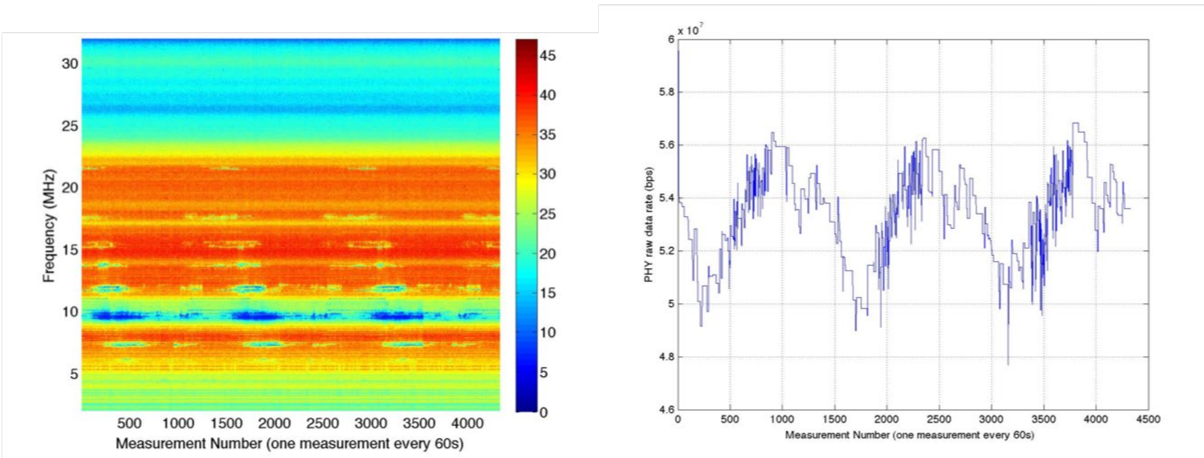


Figure 45: Long term measured SNR (left) and PHY data rate (right) with nominal data rate of 56 Mbps

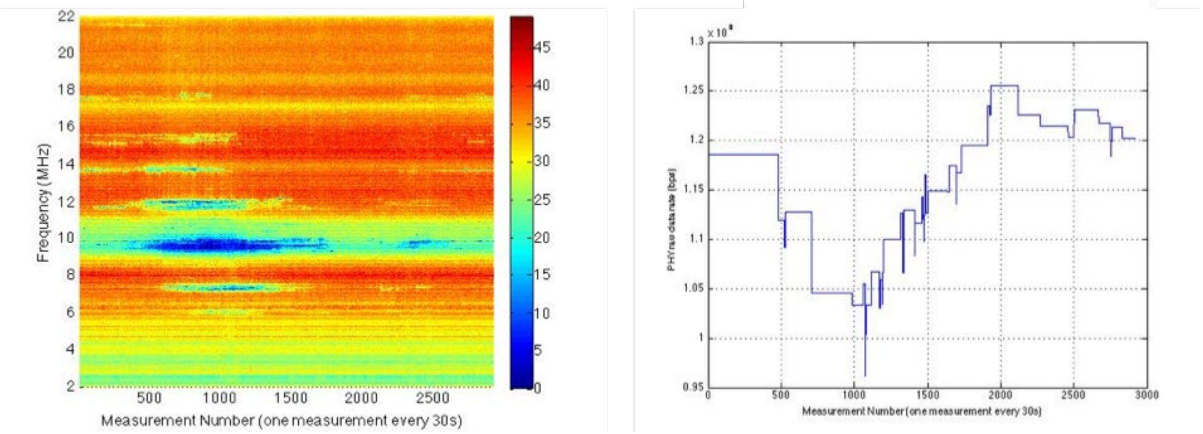


Figure 46: Long term SNR (left) and PHY data rate (right) with nominal data rate of 125 Mbps

11 Conclusion and Outlook

Worldwide increasing pressure is being placed on the electric grids and in particular the MV grids due to the steadily increasing distributed energy resources ratio. The highly time-dynamic character of such power fed into the grid by a vast amount of spatially distributed sources combined with the decreasing ratio of stabilizing rotational mass leads to substantial challenges for the future grids to keep them robust enough for the requirements and expectations of the consumers. Grids must be able to accommodate new energy flow patterns in a considerably more dynamic environment. Therefore, protection and automation systems are quickly gaining importance not only for the transmission grid but increasingly also for the distribution grid levels. The deployment of powerful concepts in the distribution grids like phasor measurement units measuring synchrophasors and line differential protection appears as a promising approach to this problem. However, the communication requirements of such applications (high availability, low latency) raise a significant challenge to the communication infrastructure as a cost-efficient solution must be provided. The use of the MV-BPL technology provides an interesting approach as it provides a cost-efficient solution in which the existing electrical grid infrastructure is used also as the communications medium.

Within a series of projects, a dedicated MV-BPL solution for mission-and-time-critical applications has been developed. The basis of this development has been the existing Power Line data bUS (PLC) BPL technology from HSLU. The PLUS technology specifically provides high reliability, low latency and deterministic behaviour. The technology has now been extended with the necessary features to support the critical requirements for PMU applications which includes:

- Accurate time-synchronization over the MV-BPL network
- Latency lower than 20 ms.

These features have been implemented, integrated and tested on a series of new modem prototypes. Extensive testing has been performed in a representative laboratory environment in order to verify the functionality and performance of these features. Results from a previous project have shown that a time synchronization accuracy of ± 250 ns per “hop” can be achieved. Within this project we have shown the maximum number of repeaters that can be achieved while still fulfilling the latency requirement (see Table 9). This number is sufficiently large in order to support typical network topologies within MV-BPL networks.

With these promising results the development of the MTC-MV-BPL solution is now completed. The solution will now be integrated and tested within a follow-up SFOE Pilot and Demonstration project which will run from January 2019 – June 2021. The project partners are HSLU, Zaphiro Technologies Sarl and BKW Energie AG. Within this project the MTC-MV-BPL solution will be evaluated against other communications technologies such as LTE, 5G and fibre optic networks in order to determine the optimal mix of technologies for the wide-scale deployment of a multi-service communications network. This evaluation will include not only a technical but also an economical comparison. The different communications technologies will be integrated and tested with PMUs (supplied by Zaphiro) and Automated Metering Infrastructure (AMI) applications in several SSs in the Wohlen bei Bern region of BKW’s MV network.

12 Publications

HSLU_1 2017 IEEE Workshop on Power Line Communications (WSPLC 2017) in Prague, Czech Republic. The title of the publication is “Channel Estimation Based on Frame Control symbol Re-encoding and Re-mapping in IEEE Std. 1901-2010.”

HSLU_2 2018 IEEE International Symposium on Power Line Communications and its Applications (ISPLC 2018). The title of the publication is “Channel Estimation Based on Frame Control Symbol Re-encoding and Re-mapping.”

HSLU_3 2018 IEEE Workshop on Signal Processing Systems in Cape Town, South Africa. The title of the publication is “FPGA Implementation of a Multi-Channel Continuous-Throughput FFT Processor.”

HSLU_4 Liset Martínez Marrero and Thomas Hunziker, "Restricted Boltzmann Machine for Interference Pattern Learning in Broadband Receivers", in Wireless Personal Multimedia Communications 2018 (WPMC'18), 2018.

13 References

[1] Sendin, Alberto, et al. "PLC deployment and architecture for Smart Grid applications in Iberdrola." Power Line Communications and its Applications (ISPLC), 2014 18th IEEE International Symposium on. IEEE, 2014.

[2] TAUPE Project Website, https://cordis.europa.eu/project/rcn/89911_en.html.

[3] Dominiak, Stephen, et al. "The application of commercial power line communications technology for avionics systems." Digital Avionics Systems Conference (DASC), 2012 IEEE/AIAA 31st. IEEE, 2012.

[4] Dominiak, Stephen; Dersch, Ulrich, “Final Report: Precise Time Synchronization of Phasor Measurement Units with Broadband Power Line Communications,” SFOE Project number SI/501392, 21.11.2017.

[5] Zimmermann, Hubert. "OSI reference model--The ISO model of architecture for open systems interconnection." IEEE Transactions on communications 28.4 (1980): 425-432.

[6] J. G. Nash, “Computationally efficient systolic architecture for computing the discrete Fourier transform,” IEEE Transactions on Signal Processing, vol. 53, issue 12, December 2005.

[7] Richard G. Lyons, “Understanding digital signal processing,” 3rd ed, Prentice Hall, 978-0-13-702741-5, August 2011, pp129-156.

[8] E. E. Jr. Swartzlander, “Systolic FFT processors: past, present and future,” IEEE 17th International Conference on Application-specific Systems, Architectures and Processors, pp. 153-158, Sept. 2006.

[9] “IEEE 1901-2010 -Standard for broadband over power line networks: medium access control and physical layer specifications,” 2011.

[10] Xilinx, “Fast Fourier transform v9.0, logic core ip product guide,” https://www.xilinx.com/support/documentation/ip documentation/xfft/ v9 0/pg109-xfft.pdf, October 2017.

[11] S. Mookherjee, L. DeBrunner, and V. DeBrunner, “A low power radix-2 FFT accelerator for FPGA,” 49th Asilomar Conference on Signals, Systems and Computers, November 2015.

[12] M. Hasan, T. Arslan, and J. S Thompson, “A delay spread based low power reconfigurable FFT processor architecture for wireless receiver,” 2003 International Symposium on System-on-Chip (IEEE Cat. No.03EX748), November 2003.
[13] Berrou, Claude, and Alain Glavieux. "Near optimum error correcting coding and decoding: Turbo-codes." Communications, IEEE Transactions on 44.10 (1996): 1261-1271.
[14] Wong CC., Chang HC. (2014) Turbo Decoder with Parallel Processing. In: Turbo Decoder Architecture for Beyond-4G Applications. Springer, New York, NY.
[15] Hosseinpour, A., Hosseinian-Far, A., Jahankhani, H. and Ghadrdanizadi, A., 2015, September. Security and Feasibility of Power Line Communication System. In International Conference on Global Security, Safety, and Sustainability (pp. 244-251). Springer, Cham.
[16] Latchman, H.A., Katar, S., Yonge, L. and Gavette, S., 2013. Homeplug AV and IEEE 1901: a handbook for PLC designers and users. John Wiley & Sons.
[17] Pittolo, A. and Tonello, A., 2014. Physical layer security in power line communication networks: an emerging scenario, other than wireless. IET Communications, 8(8), pp.1239-1247.
[18] Zhou, X., Song, L. and Zhang, Y. eds., 2013. Physical layer security in wireless communications. Crc Press.
[19] Lampe, L., 2016. Power Line Communications: Principles, Standards and Applications from multimedia to smart grid. John Wiley & Sons.
[20] Shahriar, C., La Pan, M., Lichtman, M., Clancy, T.C., McGwier, R., Tandon, R., Sodagari, S. and Reed, J.H., 2015. PHY-layer resiliency in OFDM communications: A tutorial. IEEE Communications Surveys & Tutorials, 17(1), pp.292-314.
[21] P. Koopman, K. Driscoll, and B. Hall, “Selection of Cyclic Redundancy Code and Checksum Algorithms to Ensure Critical Data Integrity,” FAA Rep., 2013.
[22] J. Wassner, S. Dominiak and J. Moya, “Model based design of an avionics power line communications physical layer,” Digital Avionics Systems Conference (DASC'15), Sept. 13-17, 2015, Prague.
[23] RTCA, “DO-254: Design Assurance Guidance for Airborne Electronic Hardware,” RTCA, Inc., Washington, DC.
[24] RTCA, “DO-331: Model-Based Development and Verification Supplement to DO-178C and DO-278A,” RTCA, Inc., Washington, DC.
[25] Sendin, A. et al., “Telecommunication Networks for the Smart Grid,” 2016.
[26] Rahman, Ashikur, and Pawel Gburzynski. "Hidden problems with the hidden node problem." Communications, 2006 23rd Biennial Symposium on. IEEE, 2006.
[27] S.-C. Lo, G. Lee, and W.-T. Chen, “An efficient multipolling mechanism for IEEE 802.11 wireless LANs,” IEEE Trans. Comput., vol. 52,no. 6, pp. 764–768, Jun. 2003.
[28] Sendin, Alberto, et al. "PLC deployment and architecture for Smart Grid applications in Iberdrola." Power Line Communications and its Applications (ISPLC), 2014 18th IEEE International Symposium on. IEEE, 2014.
[29] HSLU/SFOE, “Project Multi-Channel-PLC-Network for Cabin,” Project number BAZL 2016-069.
[30] Chakeres, Ian. "Duplicate Packet Detection for Multicast: Methods, Analysis, and Relative Performance." Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE. IEEE, 2008.
[31] Joseph Macker (editor) and the SMF Design Team, "Simplified Multicast Forwarding (SMF) for MANET," IETF Internet Draft, draft-ietf-manetsmf-05.txt, June 2007.
[32] Specification-Part, Opera. ”1: Technology.” Open PLC European Research Alliance 198.
[33] Tseng, Yu-Chee, et al. "The broadcast storm problem in a mobile ad hoc network." Wireless networks 8.2-3 (2002): 153-167.

[34] Marri, Vamsi Krishna, Stephen Dominiak, and Mikko Maurer. "Channel Modelling and Channel Selection for Broadband PLC on Medium Voltage Overhead and Underground Lines," NINTH WORKSHOP ON POWER LINE COMMUNICATIONS, 21-22 SEPTEMBER, 2015.