D 2.1/PART 2
AMENDMENT

DESCRIPTION OF CURRENT STATE-OF-THE-ART TECHNOLOGIES AND PROTOCOLS –

DESCRIPTION OF STATE-OF-THE-ART PLC-BASED ACCESS TECHNOLOGY

DUE DELIVERY DATE: -

ACTUAL DELIVERY DATE: 17.09.2010

Document History

Vers.	Issue Date	Content and changes
0.0	16.06.2010	First draft provided by EDF (PLC G3)
0.1	16.06.2010	First draft provided by ENDESA (PLC MORE)
0.2	21.06.2010	Merged G3 and MORE to single document
0.3	28.06.2010	Editorial changes
0.4	26.07.2010	Changes/improvements according to comments
0.5	13.09.2010	Final changes after TB comments
1.0	17.09.2010	Final document

Document Authors

Partners	Contributors
EDF	Gaizka ALBERDI Aline PAJOT
ENDESA	Amador GÓMEZ Manuel TELLECHEA Carmelo RODRÍGUEZ
ERSE	Diana MONETA
UKA	Martin SIGLE

Document Approvers

Partners	Approvers
DLMS UA	Gyozo KMETHY
KEMA	Gisele WIDDERSHOVEN
ELSTER	Michael ARZBERGER
IBERDROLA	Iñigo Berganza
LANDIS & GYR	Tomas SCHAUB

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY AND ACRONYMS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AES	Advanced Encryption Standard
BPSK	Binary Phase Shift Keying
CMAC	Cipher based Message Authentication
CRC	Cyclic Redundancy Check
DBSPK	Differential Binary Phase Shift Keying
DQPSK	Differential Quaternary Phase Shift Keying
EAP	Extensible Authentication Protocol
HHU	Hand Held Unit
IP	Internet Protocol
IPv6	Internet Protocol version 6
LV	Low Voltage
MAC	Medium Access control
MV	Medium Voltage
OFDM	Orthogonal Frequency Division Multiplex
OSI	Open Systems Interconnection
PHY	Physical
PLL	Phase Locked Loop
PLS	Physical Signalling
QoS	Quality of Service
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
VPN	Virtual Private Networks

REFERENCES

[EN50065] EN 50065-1, Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz, CENELEC, Brussels, 2001

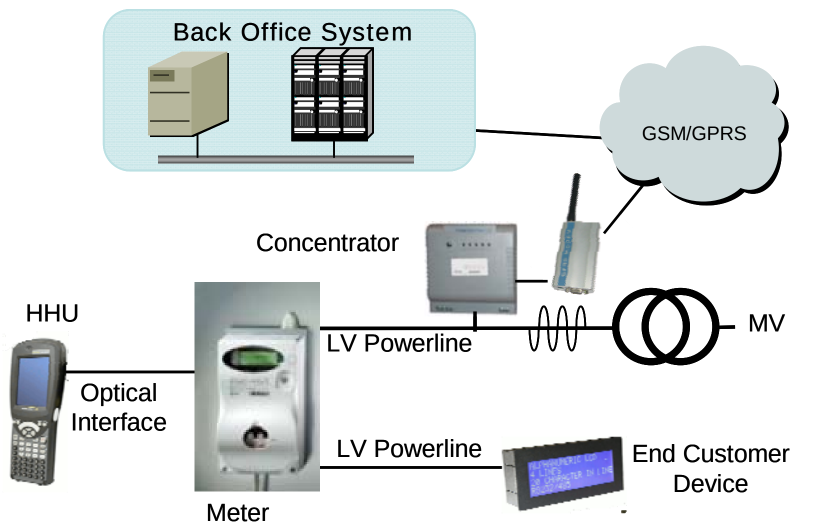
[802.15.4-2006] IEEE 802.15.4:2006, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)

[rfc4944] IETF RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. Edited by G. Montenegro, N. Kushalnagar, D. Culler. September 2007. Available from: http://www.ietf.org/rfc/rfc4944.txt

1 PURPOSE

This document is an Amendment of Part 2 of deliverable D2.1 taking into account two additional technologies, “Meters and More” and “PLC G3”.

2 Table of amendments to the core document

page	paragraph	action	amendment
93	3.3.2	Add	Add a new paragraph 3.3.2 **3.3.2 METERS AND MORE** **3.3.2.1 Overview** The Meters and More technology is an evolution of the Enel Telegestore, which is working in Italy in 35 millions of electricity meters since 2008. “Meters and More Open Technologies” no-profit Association manages the adoption, maintenance and evolution of Meters and More specification. Meters and More defines a complete solution implementing layers 1, 2 and 7 of OSI protocol stack. Main elements of the architecture are meters, concentrator and back-office system. **3.3.2.2 System architecture**  Figure 2-1 Meters and More System Architecture There are five main types of nodes foreseen for the realization of the Meters and More system and its management:

			1. **Meter (also called "A-Node"):** is a peripheral unit which can communicate, via PLC, with the Concentrator (in this case it acts as slave) or with an associated end customer device (in this case it acts as master). It's the Electricity Meter, an electronic smart-metering device with communication capability. It can be accessed with an Hand Held Unit (HHU) device via the local optical interface or remotely from the optical port of another meter via PLC. So, it can communicate (for the exchange of data) with the Concentrator, other reachable meters and (if existing) an associate end-user device. It can be remotely managed by a Back Office System, via the relevant Concentrator. It's located in the customer site. 2. **End Customer device (also called B-Node)**: is a peripheral unit which can communicate, via the associated A-Node, with the Concentrator and the Back Office System; it always acts as a slave. When available, it permits an interaction and/or display of various kinds of information to the customer. It is located in the customer site. 3. **Concentrator:** is the master (and unique) of the section of network in which is inserted. It mainly collects and manages the information received from the A-Node and from the B-Node's (if any) and transmit these informations to a Back Office site. In addition manages the communications with the meters through the PLC. Usually it's located in a sub-station of MV-LV transformation provided of a wide-area interface (e.g. a 2G+ equipment). 4. **HHU terminal**: is a terminal mainly used for installations and/or other maintenance activities of the meters via a local (optical) connection. Moreover, when connected to a meter, via the PLC, can operate on others reachable meters, for remote interventions, in a transparent way. 5. **Back Office system:** realizes the de-coupling between the legacy systems of the utilities and their field's devices; it's able to decide and adopt the right paths and adequate protocols to reach and manage any kind of device, each one with, potentially, very different features, behaviour and functionalities. The Back Office system receives work orders and commands, to accomplish a request toward the network, and sends back acknowledgments and operation's results. A

Legacy System could be a Customer Commercial System, that manages the customer's supplying contracts, as well as a Network Maintenance System, that manages alarms and maintenances of any device installed on the field. Furthermore a Customer Care System could interface the Back Office system in order to send, for example, messages related to energy supplying contract or simply to advertise the customers.

3.3.2.3 Protocol architecture for MI1-CI1, MI5 (PLC interfaces)

The set of protocols chosen to realize the communication between the equipments reaches the following objectives:

- satisfy the Application requirements in terms of efficiency and effectiveness with high level of security;
- minimize the amount of data used during the procedures of network configuration;
- efficient use of the channel.

The communication structure is based on a 3 levels stack.

3.3.2.3.1 Physical and data-link layers

For lower levels 1 and 2, the main features and the tasks performed by each protocol (and the communication disciplines) are the following ones:

- PLS sub layer protocol of PHY layer performs a modulation/demodulation PSK scheme over the Power Line. The supported modulation scheme is BPSK coded mode @ 4.800 bps.

The used communication channel is centered on 86 Khz frequency. Additionally, the Physical Layer provides bit and byte synchronization and Signal to noise ratio (SNR) estimation services;

HEADER			PAYLOAD		
Preamble	Unique Word	Mode	Size	MAC Payload	CRC32
2-5 bytes	4 bytes	1 byte	1 byte	(Size-4) bytes	4 byte

Figure 2-2 Physical frame structure

Preamble: A sequence of alternating 1 and 0 symbols required by the receiver PLL to lock on the best sampling time.

Unique Word: 4 bytes pattern on which the receiver performs:

- Frame synchronization: only after Unique Word identification, the incoming data are considered a valid message and then demodulated;
- Byte synchronization.

The pattern value is 0x014AE326.

Mode: One byte pattern delimiting the start of the convolutional coding used on the PHY payload (Size, MAC Payload, CRC32). The pattern value is 0x33.

Size: A byte counting the number of MAC Payload and the CRC32 bytes;

MAC Payload: The MAC payload, with a length (Size) ranging from 0 up to 251 bytes;

CRC32: Standard 32bit CRC calculated on fields Size and MAC Payload

- MAC sub-layer accomplishes the following main functionalities:
  - o connectionless end-to-end service between master node and all the net slave nodes;
  - o timers management of net busy condition in master nodes and repeaters;
  - o received frames filtering, on the basis of a single or grouped address;
  - o frame errors detection;
  - o phase detection;
  - o Short addressing mode. To improve the efficiency and the effectiveness of transmission over a noisy physical medium, shorter messages as possible needs. This protocol offers the capability to use a reduced node address length; this feature is mainly useful in case of communication involving several hops of repetition. The concentrator can use a two bytes address besides of a six bytes address for each meter of the communication path.

LT	ADDR	CTL	RP	NB	INF	SVT
1 byte	6 bytes	1 byte	m x 2/6 bytes	-	4-130 bytes	4 bytes

Figure 2-3 MAC frame structure

			LT: Frame Length: this field is composed by 1 byte and it indicates the length of the frame, starting form ADDR field until SVT field. **ADDR**: The field is composed by 6 bytes and it contains: o MAC address of destination node (repeater or final node) in the upstream frames; o MAC address of source node (final node or repeater) in the downstream frames. **CTL**: Control field: it identifies the frame function **RP**: Repetition Parameters. This field contains information about the communication path to the final node. **NB**: Used for future implementations. **INF**: This field is composed by a variable integer number of bytes; information (MAC-sdu) that has been end-to-end exchanged between master and slave, is contained inside this field. **SVT**: Frame Checking Sequence (CRC). This field contains the reminder (CRC of 32 bit; first bit transmitted = most significant bit), complemented to ones, of the division (modulo 2) of the bits sequence contained between the fields LT and SVT (considering, in this sequence, the first 32 bits starting from LT as complemented to ones) for the following generator polynomial: $g(x) = x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x+1$ LLC layer performs the following functions: o execution of end-to-end exchange procedures to guarantee a correct access procedure that avoids any possible collision on the net; o indication to application net availability, in the sub-net master node; user can request transmission of another message, upon reception of this indication; o re-transmissions management on exchanges with expected answer in the master nodes. o encryption mode indication (see LSAP field description). The message exchange is encrypted using the following algorithms: ▪ AES-ECB encryption – “Block” (128 bits) encryption by AES-ECB algorithm, using a key “K” of 128 bits;

- AES-CTR encryption – "Stream" encryption by AES-CTR algorithm, using a key "K" of 128 bits;

CONTROL	LSAP	DATA
1 byte	1 byte	App SDU length

Figure 2-4 LLC frame structure

CONTROL: Control field see IEC 61334-4-32

LSAP: (1 byte) is better defined considering 2 Nibble identified as DSAP and SSAP (2 * 4 bits):

DSAP: (Destination service access point)

Bit 0-1 used to identify application or network management

Bit 2-3 available

SSAP: (Source service access point) is used to discriminate what kind of encryption method is used to protect the payload field.

SSAP coding:

0000 Encryption disabled

xx10 Encryption AES ECB

xx01 Encryption AES CTR

x0xx Encryption uses READ key

x1xx Encryption uses WRITE key

Meters and More application layer is a set of different application layer protocols depending on the interface used for the involved devices connection.

3.3.2.3.2 Application Layer

In this Application Layer protocol the following activities are supported:

· Network management commands messages exchange. This activity permits concentrator to perform network management operations as the automatic nodes discovery and recovery.

· Parameters programming. This activity permits to activate customer's supply, to customize its contract parameters (tariff and so on) and to stop it. Furthermore this activity permits to manage the field device's configuration to optimize the execution of service routines (virtual data set creation and so on). Messages of this activity can be in the authenticated or unauthenticated mode.

· Data exchange. This activity permits to read data through the specification of tables and parameters coordinates. Messages of this activity can be in the authenticated or unauthenticated mode.

· Software downloading. This activity permits to update network device's software.

· Acknowledgements exchange. Messages of this activity are used by A-Nodes and B-Nodes to communicate to concentrator that received commands have been (un)correctly received and executed.

· Data exchange between a Meter and the associated End Customer device.

· Commands messages exchange. This message permit to a concentrator to execute some special operations on a network node (node reset, status word locking and so on). Messages of this activity can be in the authenticated or unauthenticated mode.

· Security management. An high level of security is ensured using authentication and "playback attack" protection. The message exchange is authenticated using AES-CMAC algorithm, using a key "K" of 128 bits. AES-CMAC generates a fixed length signed "digest" of 128 bits;

Protection against "playback attack" is realized implementing a messages implied numbering.

Message Code	Message Data		DATE-TIME	DIGEST
	IDEN	Data		

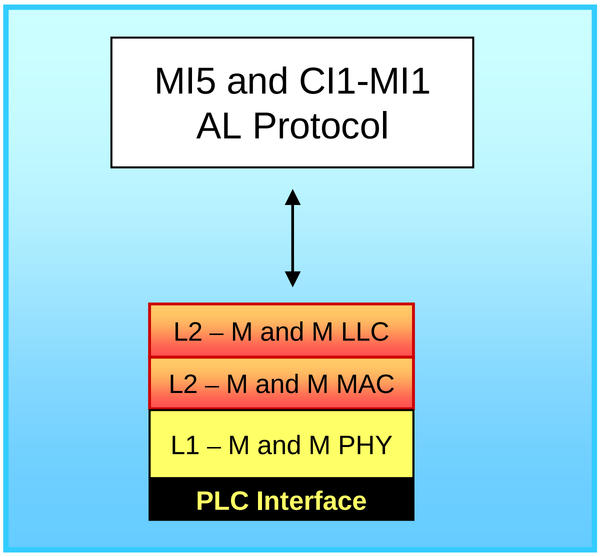
Figure 2-5 Application Message format for authenticated mode

Message Code: Message Identifier (it indicates if the message have to be authenticated or not) [1 byte]

Message Data: [variable length] it is composed by:

IDEN: a list of registers identifiers involved in the operation specified in the Message code

Data: a list of values to be written or a list of read

			values. [it's present only in case of writing / responses messages] **Date-Time**: [8 bytes] Time stamp. [it's present only in case of authenticated message] **Digest**: [8 bytes] AES CMAC signed "digest". [it's present only in case of authenticated message] Following figure shows the configuration of protocol stack for MI1-CI1 and MI5 interfaces.  Figure 4.6 Protocol stack for MI1-CI1 and MI5 interfaces
93	3.3.3	Add	Add a new paragraph 3.3.3 **3.3.3 PLC G3** **3.3.3.1 General overview** Designed for large-scale utility infrastructures, PLC G3 solution includes OFDM-based PHY/MAC layers and a 6LoWPAN adaptation layer to transmit IPv6 packets over the powerline. Advanced modulation enables a robust data rate in extremely harsh power line channels both in LV and MV grids, cohabitation with S-FSK technology, and adaptive tone mapping to avoid interfering frequencies. Reliable data rate communications can be maintained over the long distances

			required by smart grid infrastructures.

The PLC G3 solution offers:

- A robust high-performance PHY layer, based on OFDM and adapted to the PLC environment within the CENELEC A band.
- A MAC layer of the IEEE 802.15.4 type, well suited to low data rates
- A 6LoWPAN adaptation layer, fully compatible with IPv6, the new generation of IP (Internet Protocol), which widely opens the range of potential applications and services
- Embedded functionalities for the DLMS/COSEM Metering Application layer (IEC 62056-53, IEC 62056-61 and IEC 62056-62)
- A coherent security approach based on the widely available security mechanisms and algorithms

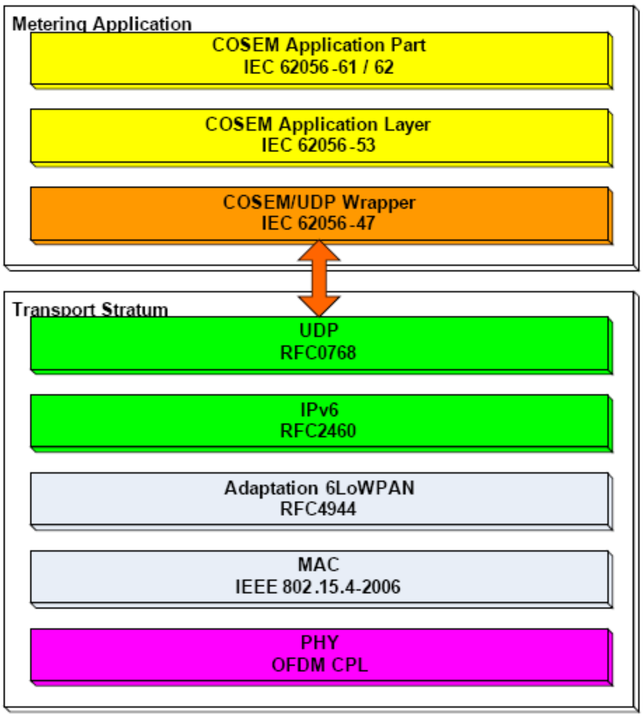
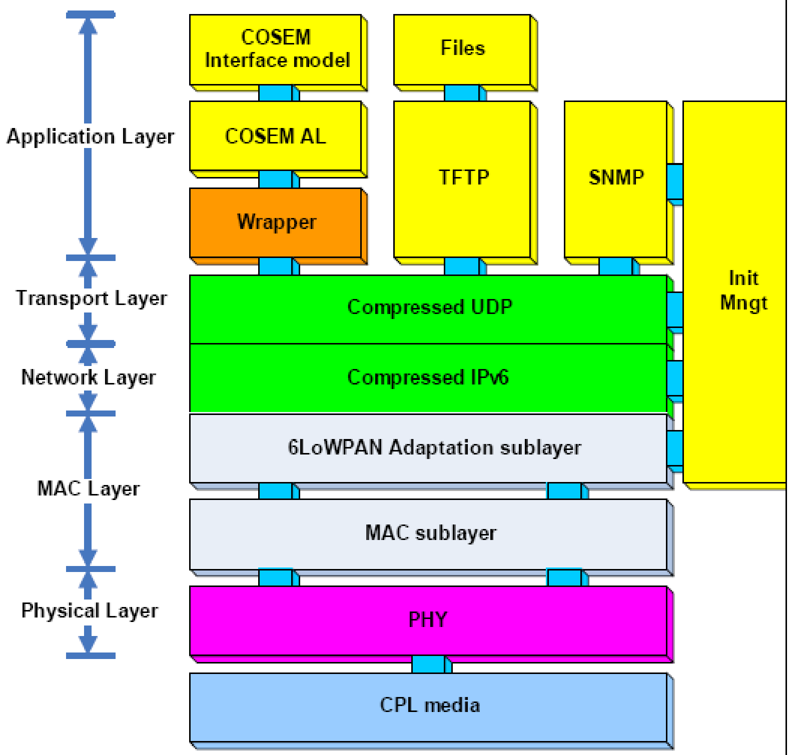


Figure 2-6 PLC G3 profile

3.3.3.2 Architecture of the system

			The G3 OFDM PLC (Orthogonal Frequency Division Multiplexing - Power Line Carrier) specifications are developed to meet the following aims: • Robustness: the communication profile must be suited to severe environments • Performance: it must take full advantage of the CENELEC A band • Simplicity: it must be simple to implement, install (Plug and Play), operate and maintain • Flexibility: it must be compatible with diverse applications and network topologies. • Security: it must offer a safe environment for the promotion of Value Added services • Openness: it must be based on open standards in order to support multi-supplier solutions. • Compatibility: it must be able to function in a given network with earlier metering systems and existing metering applications • Scalability: it must support all future metering developments. To this end, the OFDM PLC protocol stack aggregates several layers and sublayers that form the PLC G3 profile: • A robust high-performance PHY layer, based on OFDM and adapted to the PLC environment (CENELEC band A). • A MAC layer of the IEEE type, well suited to low data rates • IPv6, the new generation of IP (Internet Protocol), which widely opens the range of potential applications and services • And to allow good IPv6 and MAC interoperability, an Adaptation sublayer taken from the Internet world and called 6LoWPAN. • A metering application layer based on the

			DLMS/COSEM IEC standards. The following figure gives an overall view of the OFDM PLC Communication Profile:  Figure 2-7 PLC G3 Communication profile The figure below gives the general format of the frames. It shows the headers for all the levels of the Transport layer (PHY, MAC, Adaptation 6LoWPAN, compressed IPv6 and compressed UDP):

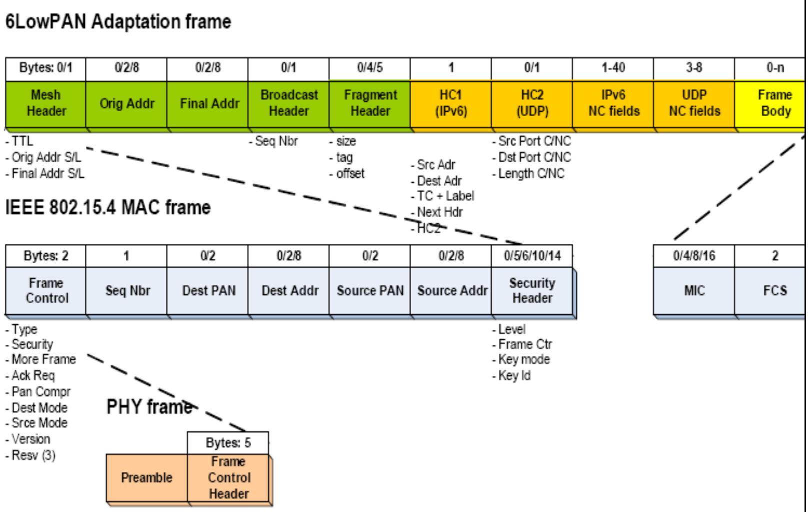


Figure 2-8 General format of the frames

3.3.3.3 *Physical (PHY) Layer*

The PLC G3 PHY layer is designed to transmit and receive over power lines both in LV and MV. PLC G3 is based on adaptively modulated Orthogonal Frequency Division Multiplexing (OFDM), along with forward error correction, Reed-Solomon coding and data interleaving.

The PLC G3 PHY layer provides a robust and high-performance OFDM modulation scheme, perfectly adapted to the PLC environment within the CENELEC A band constraints, coping with severe channel conditions, wide range of noises as well as narrowband interferences.

The PLC G3 PHY layer specification address the following main objectives:

1. Provide robust communication in extremely harsh power line channels

2. Provide a minimum of 20kbps effective data rate in the normal mode of operation

3. Ability to notch selected frequencies, allowing the cohabitation with S-FSK narrow band communication.

4. Dynamic tone adoption capability to select frequencies on the channel that do not have major interference , thereby ensuring a robust communication

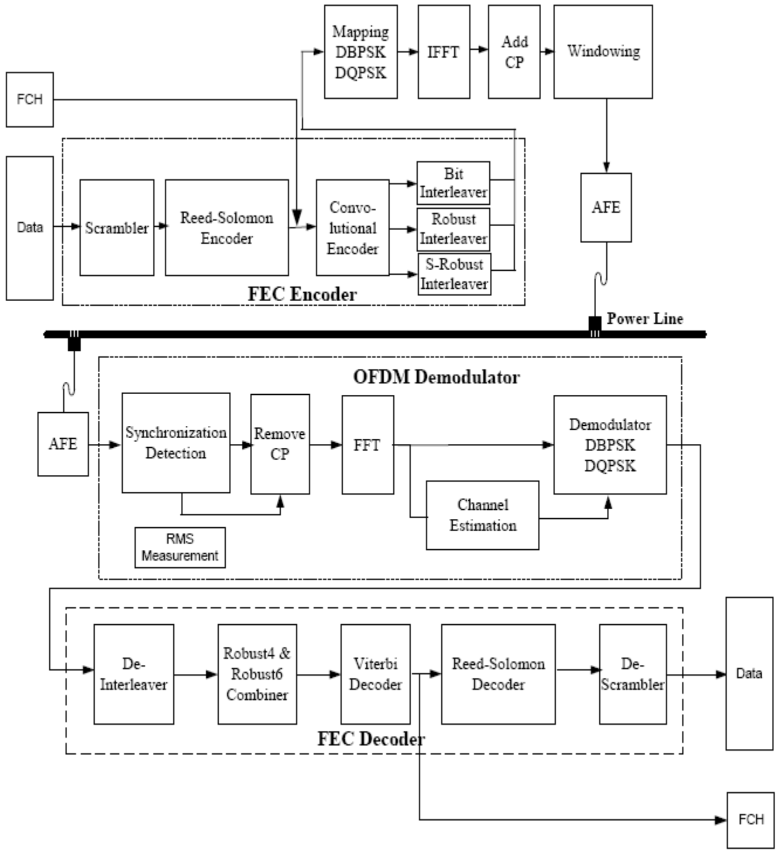


Figure 2-9 Block diagram of the PLC G3 Transceiver

The PLC G3 supports the portion between 35.9kHz to 90.6kHz of the CENELEC-A band [EN50065]. An OFDM with DBPSK and DQPSK modulation schemes per carrier is selected to support up to 33.4kbps data rate in Normal mode of operation. The DBPSK and DQPSK modulation for each carrier makes the receiver design significantly simpler since no tracking circuitry is required at the receiver for coherently detecting the phase of each carrier.

	Number of Carriers	First Carrier (kHz)	Last Carrier (kHz)
CELENEC A	36	35.938	90.625

Figure 2-10 Number of carriers for various bands

A total of 36 data subcarriers are transmitted between 34 kHz and 90 kHz, adaptively using one of three differential digital modulation schemes (ROBUST mode, DBPSK, DQPSK).

In ROBUST mode DBPSK is used and additional each bit is repeated four times making the system more robust to channel impairments. At the same time the throughput is reduced by about factor of 4.

CENELEC A Number of Symbols	Data Rate (DQPSK) bps P16*	Data Rate (DBPSK) bps P16*	Data Rate (Robust) bps P8**
12	13453	4620	N/A
20	20556	8562	N/A
32	27349	12332	N/A
40	30445	14049	3192
52	33853	15941	3765
56	34759	16444	3867
112	N/A	20360	5002
252	N/A	N/A	5765

Figure 2-11 Data rate for various Modulations (including FCH)

3.3.3.4 *MAC Layer*

3.3.3.4.1 Overview

The PLC G3 MAC layer specification comprises two sublayers:

- The MAC sublayer derived directly from the MAC part of [802.15.4-2006]
- And the 6LoWPAN Adaptation sublayer derived directly from 6LoWPAN such as it is defined by [rfc4944] and the associated documents.

The IEEE 802.15.4-2006 is the standard which specifies the media access control for low-rate wireless personal area networks. It is maintained by the IEEE 802.15 working group.

It is the basis for the ZigBee, WirelessHART, MiWi and PLC G3 specifications. Furthermore, it is perfectly suited to be used with 6LoWPAN and standard Internet protocols, as it is the case for PLC G3. The emphasis of the combination of IEEE 802.15.4 and 6LoWPAN layers results in low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power

			consumption even more. In the following subsections brief descriptions of the selections and extensions used in G3 PLC compared to IEEE 802.15.4.2006 [802.15.4-2006] and IETF RFC 494 [rfc4944] are given. *3.3.3.4.2 IEEE 802.15.4* The IEEE 802.15.4 proposes to have two types of network: beacon and non-beacons. The choice has been done to use a non-beacon network. Thus, the PLC G3 network is not synchronized and uses only the CSMA-CA algorithm. Furthermore, the contention-free Guaranteed Time Service (GTS) is not implemented. For the PLC G3 coordinator (PAN coordinator), the management of the network is simpler and request less resource than a beacon network. It's important to note that for neighbour discovery mechanism, the beacon frames are used. In IEEE 802.15.4 standard two types of devices are defined: Full function devices and reduced function devices. In PLC G3 every device is a full function device. PLC G3 introduces some selections and extensions on the channel access procedure: • Interframe (IFS) spacing has been modified to introduce a contention state to improve the real-time behaviour. This is used to have a prioritized access on frame transmission, • No super-frame is used (due to non-beacon network type selection), • As specified in IEEE 802.15.4 only the unslotted version of the CSMA-CA algorithm is supported, • For acknowledgment a classical ARQ mechanism is used. It's important to note that, to use the available bandwidth efficiently, the acknowledgment is done at physical level and not at MAC level. This is an enhancement compared to IEEE 802.15.4. One more important point is that the association and disassociation procedures are not done at MAC level but at 6LoWPAN level (use of 6LoWPAN Bootstrap Protocol described in PLC G3 specifications). Thus, one consequence

is that only the active scan procedure is implemented in PLC G3 protocol.

PLC G3 supports only the beacon command frame. PLC G3 specifies a new command frame: Tone Map Response. This is used for the adaptive tone mapping procedure. This procedure is new compared to the current specification of IEEE 802.15.4. In addition of the physical layer specificities this procedure permits the PLC G3 technology to cross the transformer. It is important to note that this procedure introduces some dependency between the PHY and the MAC mainly due to the Tone Map Request procedure (e.g. new bit in the FCH of the PHY frame). This procedure permits to adapt the OFDM modulation (carriers to use) and the transmit power according to the quality of the received signal.

About security at IEEE 802.15.4 level, only the ENC-MIC-32 mode is allowed by the PLC G3 specifications. Each MAC frame exchanged is ciphered (using CCM type) to ensure low layer confidentiality and integrity. Security feature is optional and may be activated or not.

3.3.3.4.3 RFC 4944 – 6LoWPAN

In PLC G3 no IPv6 prefix learning mechanism is implemented. Thus, the LAN PLC G3 remains local with routable address to internet for instance.

To introduce the MESH topology and the 6LoWPAN bootstrapping protocol (used for the association / disassociation procedures) a new 6LoWPAN header called command frame header is added. This header is used to carry the routing messaging specified in the LOAD protocol.

For PLC G3 network management and diagnostic, the route discovery procedure has been added by using two new types of message (Path Request and Path Reply).

Some enhancements of the 6LoWPAN bootstrapping protocol on mechanism and on message contents (more precisely on EAP message contents) have been specified.

For authentication Extensible Authentication Protocol (EAP) is only used with EAP-PSK (Pre-shared key). The hierarchy of the keys used in the PLC G3 is described in the specification.

The adaptation layer and the primitives associated are added to the PLC G3 specifications. This is due to the fact that no primitive is currently defined by the IETF.

			3.3.3.5 Benefits of IP protocol for Smart Metering Since the PLC G3 technology is inherently based on IPv6, it offers several advantages concerning the management and maintenance of the system. There is a growing trend towards the use of TCP/IP technology as a common communication platform for Smart Metering applications, so that utilities can deploy multiple communication systems, while using IP technology as a common management platform. To support the large number of emerging applications for smart metering, the underlying networking technology must be inherently scalable, interoperable, and have a solid standardization base to support future innovation as the application space grows. IP has proven itself a long-lived, stable, and highly scalable communication technology that supports both a wide range of application, a wide range of devices, and a wide range of underlying communication technologies. The layered architecture of IP provides a high level of flexibility and innovation. Over the past 20 years, IP has evolved to support new mechanisms for high availability, enhanced security, support of Quality of Service (QoS), real-time transport, and Virtual Private Networks (VPNs). IP provides standardized, lightweight, and platform-independent network access for smart metering purposes as well as other embedded networked devices. The use of IP makes devices accessible from anywhere and from anything. PLC G3 technology takes into account the advanced features of the IP and uses SNMP protocol for Management, TFTP protocol for file transfer and proven QoS and Security features widely deployed in the Internet world.
NOTE: Figure captions and the table of content has to be updated in order to take into account the previously described amendments			

Table 2-1 Amendments to D 2.1/Part 2

4 Copyright