

**note interne**

**Metering Department**



## Linky PLC profile functional specifications

Identification: ERDF-CPT-Linky-SPEC-FONC-CPL

Version: V1.0

Number of pages: 40



### • Summary

This document deals with the use of Linky Profile elements, and gives the implementation items that interest both the application programmers and the users.

### • Associated document(s) and appendix (appendices)

### • Document history

Version	Application date	Type of modification	Cancel and replaces
V1.0	30/09/2009	Original document	

### • Accessibility

<input type="checkbox"/> General	<input type="checkbox"/> ERDF Électricité Réseau Distribution France	<input type="checkbox"/> Restricted	<input type="checkbox"/> Confidential
----------------------------------	--	-------------------------------------	---------------------------------------

### • Addressee(s)

### • Validation

Written by		Checked by		Approved by		
Name - Department	Initials	Name - Department	Initials	Name - Department	Initials	Date
Linky Equipment Department		Martial Monfort		Jean-Marie Bernard Jean Vigneron		

**CONTENTS**

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1 Document positioning .....	4
1.2 Overview of the Linky PLC system .....	4
1.3 Reference documents.....	5
1.4 Normative references .....	6
<b>2. PLC PROTOCOL PRINCIPLES.....</b>	<b>7</b>
2.1 Reference model .....	7
2.1.1 Reference model for the Linky concentrator .....	7
2.1.2 Reference model for the Linky meter .....	9
2.1.3 Reference model for existing meters.....	10
2.2 Physical layer .....	11
2.2.1 Modulation/demodulation description .....	11
2.2.2 Signal and noise level measurement.....	13
2.2.3 Physical synchronisation .....	14
2.3 Link layer.....	15
2.3.1 MAC layer.....	15
2.3.2 Description of the Search Initiator function on the MAC layer of the Server .....	15
2.3.3 Description of the MAC layer for repeating a frame consisting of a subframe .....	16
2.3.4 Description of the MAC layer for a frame consisting of one subframe .....	18
2.3.5 Description of the MAC layer for a frame consisting of two subframes.....	20
2.3.6 Description of the MAC layer for a frame consisting of n subframes .....	21
2.3.7 LLC layer .....	22
2.4 Application layer.....	22
2.4.1 DLMS Application layer .....	22
2.4.2 COSEM application layer .....	23
2.4.3 Correspondence between the MIB and COSEM classes for the PLC.....	23
2.4.4 CIASE.....	25
2.4.5 Alarm management .....	26
<b>3. PLC FUNCTIONS ASSOCIATED WITH A METER .....</b>	<b>29</b>
3.1 Physical synchronisation.....	29
3.2 PLC and Timeout states .....	30
3.2.1 PLC states .....	30
3.2.2 Timeouts.....	30
3.2.3 State changes.....	31
<b>4. PLC FUNCTIONS ASSOCIATED WITH A CONCENTRATOR .....</b>	<b>32</b>

## Linky PLC profile functional specifications

4.1	Management of PLC communication modules.....	32
4.2	Equipment identification.....	32
4.3	Discovery function.....	32
4.4	Description of the registration process .....	33
4.4.1	For a new module (Server).....	33
4.4.2	For the concentrator (INITIATOR).....	33
4.5	Credit management .....	35
4.6	Calculating the Timeout between two requests .....	36
4.7	Disappearance, loss of module/meter .....	37
4.8	Crosstalk management.....	37
4.8.1	Smart synchronisation.....	37
4.8.2	Repeater cluster management.....	37
<b>5.</b>	<b>PLC COMMUNICATION SECURITY .....</b>	<b>39</b>
5.1	Encryption method .....	39
5.1.1	Initialisation vector.....	39
5.2	"CCC" secret key .....	39
5.3	Unique "CC_LAN" and "CC_LOCALE" keys.....	40
5.4	Session keys.....	40
5.4.1	LAN interface.....	40
5.4.2	LOCAL interface with encryption.....	40
5.4.3	LOCAL interface without encryption.....	40

## 1. INTRODUCTION

### 1.1 Document positioning

The aim of the PLC protocols implemented for the Linky project is to allow a Client device (the concentrator) to communicate with the Server devices (the meters) by using the services defined by the COSEM or DLMS application layer over a PLC network infrastructure.

- The COSEM application layer is defined by the IEC 62056 series of standards and its extensions described in the DLMS UA Books, [13] and [14].
- The DLMS application layer and the lower layers of the PLC protocol are defined by the subset of the IEC 61334-4 standards.
- This communication objective also includes network management, using the services provided by the CIASE layer described in IEC 61334-4.

The above-mentioned protocol base is supplemented by new services, which are deemed to be extensions to the standard.

Document ERDF-CPT-Linky-SPEC-PROFIL-CPL ("Spécifications du profil CPL Linky" (Linky PLC profile specifications)) describes the selected normative elements and the recommended extensions.

This document ERDF-CPT-Linky-SPEC-FONC-CPL ("Spécifications fonctionnelles du profil CPL Linky" (Linky PLC profile functional specifications)) describes how to use these elements and explains how they can be implemented by users (application developers and operators), as opposed to the previous document, which is of more interest to developers of "protocol elements" (or protocol "stacks").

### 1.2 Overview of the Linky PLC system

The Linky PLC system consists of:

- Single-phase and three-phase Linky meters incorporating a PLC communication interface,
- PLC modules with a Euridis interface for "Yellow tariff" meters,
- PLC modules with a serial interface for "PME/PMI" type meters,
- Concentrators installed in the MV/LV transformer stations,
- The Linky central IS, which controls the PLC communication modules, meters and concentrators and implements the various services.

Later in this document, the "PLC module" concept combines both the PLC part of a meter incorporating the PLC communication function and the BCPLs.

However, each of these "PLC modules" has a different communication profile. These profiles are as follows:

- The Linky Server profile: integrated with the single-phase and three-phase meters.
- The PLC module Server profile: PLC modules with a Euridis interface (see [16]).
- The PME/PMI Server profile: PLC modules with a serial interface for PME/PMI meters (see [A3]).

In each Server profile, we distinguish between information which applies to the lower layers, Network management-related services and Meter application-related services. The following table summarises the services used by the Server profiles.

## Linky PLC profile functional specifications

Server profile	Lower layers	Network management	Application
Linky meter	Physical and MAC layer 2400 Baud LLC layer	CIASE	COSEM SN application layer (+ block read, block write, multi-references, read parameter + security)  Object definition (OBIS and Interface Class)  The MIB objects are replaced with the PLC Setup classes
PLC module	Physical and MAC layer 2400 Baud LLC layer	CIASE MIB (DLMS Application layer)	DLMS Application layer
PME/PMI meter	Physical and MAC layer 2400 Baud LLC layer	CIASE MIB (DLMS Application layer)	DLMS Application layer (+ detailed access)

The concentrator communicates automatically via carrier current over the low-voltage distribution network with all the Linky meters and all the PLC modules connected to this network. It also communicates with the meters connected to the Euridis interfaces and the serial interfaces via the various PLC modules.

Client profile	Queried Server profile	Lower layers	Network management	Application
Linky concentrator	Linky meter	Physical and MAC layer 2400 Baud LLC layer	CIASE	COSEM SN application layer (+ block read, block write, multi-references, read parameter + security)  Object definition (OBIS and Interface Class)  The MIB objects are replaced with the PLC Setup classes
	PLC module	Physical and MAC layer 2400 Baud LLC layer	CIASE MIB (DLMS Application layer)	DLMS Application layer
	PME/PMI meter	Physical and MAC layer 2400 Baud LLC layer	CIASE MIB (DLMS Application layer)	DLMS Application layer (+ detailed access)

### 1.3 Reference documents

- [A1] ERDF-CPT-Linky-SPEC-PROFIL-CPL Spécifications du profil CPL Linky (Linky PLC profile specifications)
- [A2] HR-43/04/027/A Cahier des charges du Boitier CPL pour le relevé des compteurs (BCPL meter measurement specifications)
- [A3] H-R43-2007-00131-FR Spécifications du compteur PME/PMI (CPL): Serveurs DLMS du compteur PME-PMI (PME/PMI (PLC) meter specifications: DLMS Servers for the PME-PMI meter)

## 1.4 Normative references

The PLC system conforms to the following standards:

- [1] IEC 61334-4-1:1996, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4: Protocoles de communication de données – Section 1: Modèle de référence du système de communication (Distribution automation using distribution line carrier systems – Part 4: Data communication protocols - Section 1: Reference model of the communication system)
- [2] IEC 61334-4-32:1996, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4: Protocoles de communication de données – Section 32: Couche liaison de données – **Contrôle de liaison logique (LLC)** (Distribution automation using distribution line carrier systems – Part 4: Data communication protocols - Section 32: Data link layer - **Logical link control (LLC)**)
- [3] IEC 61334-4-41:1996, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4: Protocoles de communication de données – Section 41: Protocoles d'application – **Spécification des messages de ligne de distribution** (Distribution automation using distribution line carrier systems – Part 4: Data communication protocols - Section 41: Application protocols - **Distribution line message specification**)
- [4] IEC 61334-4-42:1996, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4: Protocoles de communication de données – Section 42: Protocoles d'application – **Couche application** (Distribution automation using distribution line carrier systems – Part 4: Data communication protocols - Section 42: Application protocols - **Application layer**)
- [5] IEC 61334-4-511:2000, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4-511: Protocoles de communication de données – Administration de systèmes – **Protocole CIASE** (Distribution automation using distribution line carrier systems – Part 4-511: Data communication protocols – Data communication protocols - Systems management - **CIASE protocol**)
- [6] IEC 61334-4-512:2000, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 4-511: Protocoles de communication de données – Administration de systèmes – **Management Information Base(MIB)** (Distribution automation using distribution line carrier systems – Part 4-511: Data communication protocols – Systems management – **Management Information Base (MIB)**)
- [7] IEC 61334-5-1:2001, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 5-1: **Profils des couches basses** – Profil S-FSK (modulation pour saut de fréquences étalées) (Distribution automation using distribution line carrier systems – Part 5-1: **Lower layer profiles** - The spread-frequency shift keying (S-FSK) profile)
- [8] IEC 62056-53 Ed.2:200X, Electricity metering – Data exchange for meter reading, tariff and load control – Part 53: **COSEM Application layer**
- [9] IEC 62056-61 Ed.2:200X, Electricity metering – Data exchange for meter reading, tariff and load control – Part 61: **OBIS Object identification system**
- [10] IEC 62056-62:200X Ed.2, Electricity metering – Data exchange for meter reading, tariff and load control – Part 62: **Interface objects**
- [11] IEC 61334-6:2000, Automatisation de la distribution à l'aide de systèmes de communication à courants porteurs – Partie 6: **Règles d'encodage A-XDR** (Distribution automation using distribution line carrier systems – Part 6: **A-XDR encoding rules**)
- [12] CENELEC EN50065-1/A1 May 2002 Transmission de signaux sur les réseaux électriques basse-tension dans la bande de fréquences de 3kHz to 148 kHz (Signalling on low-voltage electrical installation in the frequency range 3 kHz to 148 kHz. Part 1: General requirements, frequency bands and electromagnetic interference)
- [13] Cosem Blue Book DLMS UA 1000-1:2008 9th edition
- [14] Cosem Green Book DLMS UA 1000-2:2008 7th edition
- [15] IEC EN50065-7 Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz. Equipment impedance
- [16] IEC EN62056-31 Ed.1 Electricity metering - Data exchange for meter reading, tariff and load control

## **2. PLC PROTOCOL PRINCIPLES**

### **2.1 Reference model**

The model is based on a "contracted" three-layer architecture that provides sufficient addressing features and functions for carrier current applications, such as the Linky project.

This architecture has been built to ensure high efficiency at low communication speeds (2400 bits/s) and for high propagation delay times due to the poor quality of the distribution network as a data transmission channel. It also provides a high degree of automation for the network management functions.

To meet the requirements of all the equipment already installed and future Linky meters, the reference models are as follows:

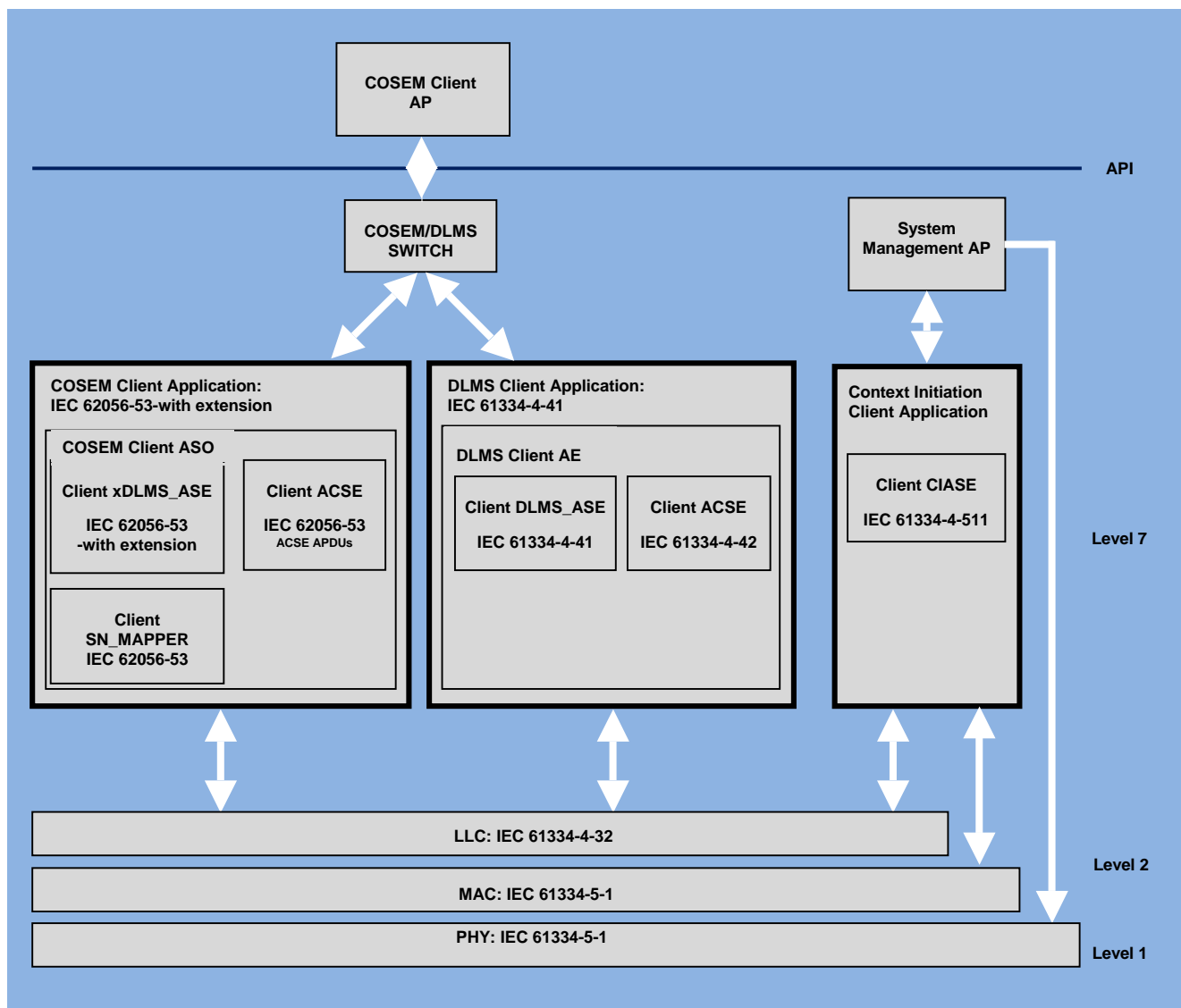
- Reference model for the Linky concentrator
- Reference model for the Linky meter
- Reference model for existing meters (see [A3])

The PLC data and its default values are described in the functional specifications for each PLC device.

#### **2.1.1 Reference model for the Linky concentrator**

The Linky concentrator reference model is illustrated in the following figure:

## Linky PLC profile functional specifications



This reference model defines a "System Management" application process (SMAP) for managing physical equipment on the network, together with two different application processes for accessing meters using the DLMS or COSEM application layers. This ensures that the concentrator is compatible with the existing equipment.

The DLMS application process controls access to existing meters such as yellow meters and PME/PMI meters via PLC modules.

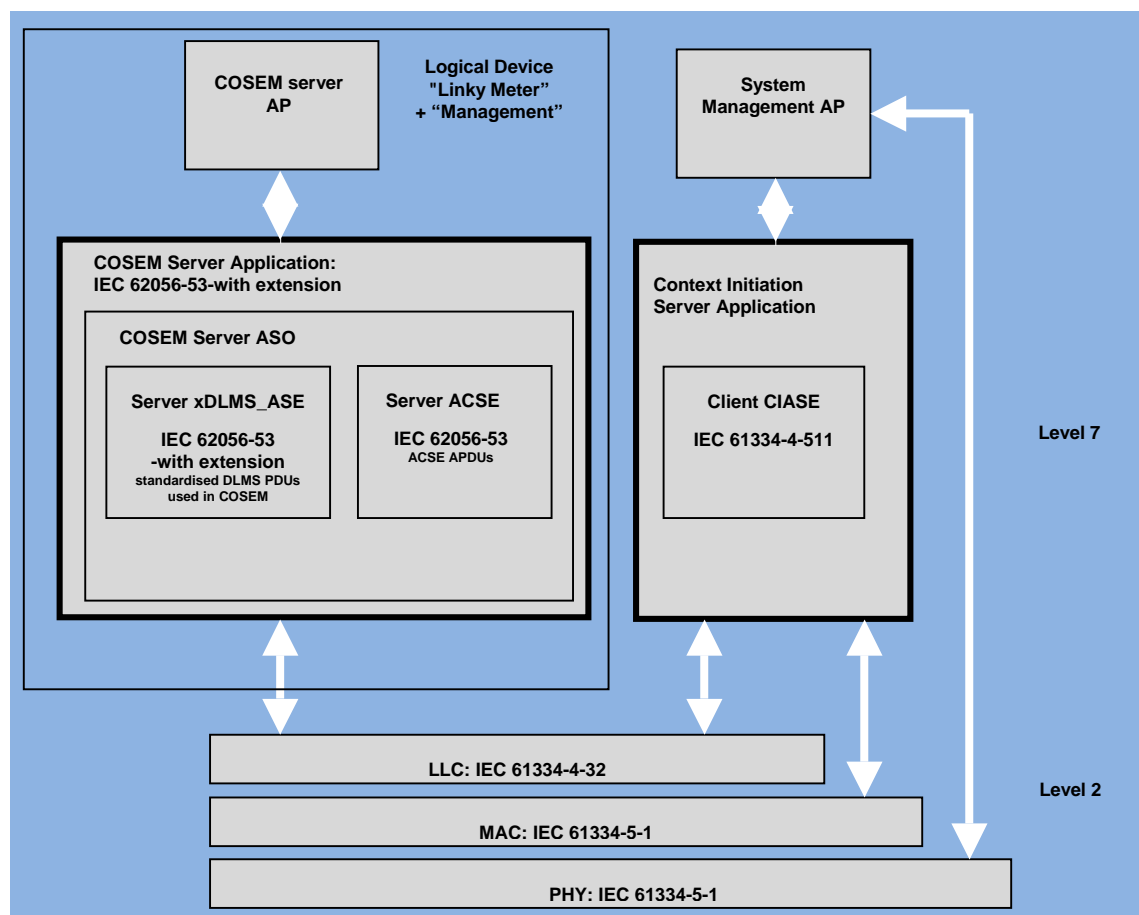
The COSEM application controls access to the Linky meters.

The Linky concentrator will provide the various COSEM Clients with a single set of services using Logical Name referencing (GET, SET, ACTION). In view of the profile of the Servers defined (see 2.1.2 and 2.1.3), where only ShortName referencing is supported (optimised communication times to ensure the required quality of service), the Linky concentrator will support at least the standard DLMS PDUs used in COSEM, but should be easily upgradeable to support all the PDUs using Logical Name referencing. It must be possible to configure the LogicalName to ShortName transfer (SN\_MAPPER) to allow the concentrator to adapt quickly to changes that may be made to a meter (modification, addition of objects).

## 2.1.2 Reference model for the Linky meter

A single "Linky meter" Logical Device is defined in the Linky meter. This logical Device contains all the metering data and includes the compulsory "Management" Logical Device on each COSEM physical device (see [8] section 6.3.1).

The Linky meter reference model is illustrated in the following figure:

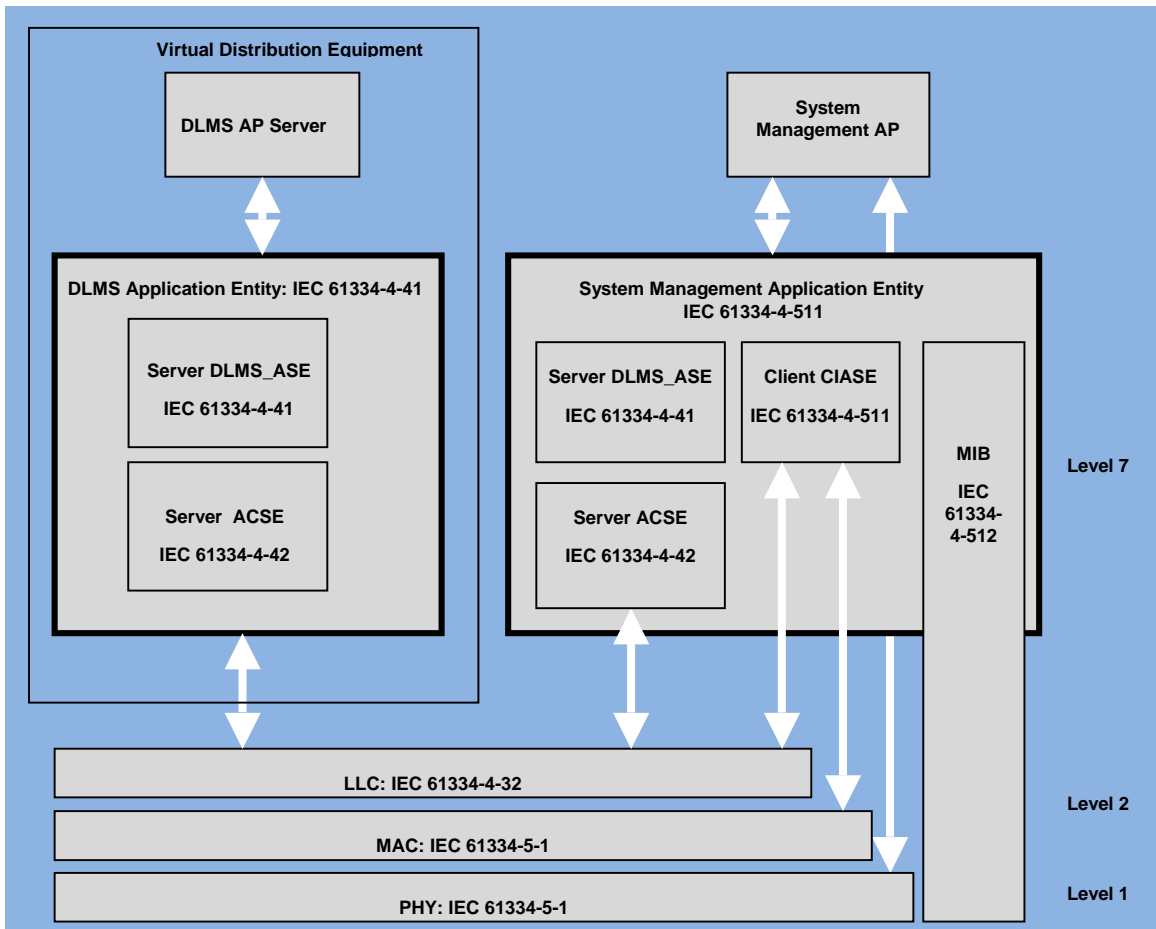


Access to the different objects of the Logical Device is conditioned by the type of Client that accesses it:

- Public Client (Application Association in non crypted ShortName mode) for read access to the "Management" Local Device objects and for programming (writing) the "Linky Meter" Logical Device CCU object.
- Client R/W (Application Association in crypted ShortName mode) for read/write access to authorised "Linky Meter" Logical Device objects.
- Broadcast / Multicast Client (Application Association in crypted ShortName mode) for access (write) in broadcast mode to authorised "Linky Meter" Logical device objects.

### 2.1.3 Reference model for existing meters

The reference model for the existing meters is illustrated in the following figure:



## 2.2 Physical layer

The physical layer defines the method of transmission (type of modulation) used for transmitting information over the physical channel, i.e. the low-voltage electrical distribution network.

The type of modulation used is S-FSK (spread-frequency shift keying).

S-FSK modulation is a modulation/demodulation technique combining some of the advantages of a conventional spread-spectrum system (for example, jammer immunity) with those of a conventional FSK system (relatively non-complex, optimised implementation).

The physical layer conforms to the following standardisation documents:

- CENELEC EN 50065-1/A1 [12], which defines the transmission bands and the rules, in order to limit mutual influence between signal transmission equipment in electrical installations and between such equipment and other equipment.
- IEC 61334-5-1[7], which defines the rules and the performances expected from an S-FSK modulator/demodulator.

The physical layer must implement the services specified in the extension to the standard (described in the document [A1]):

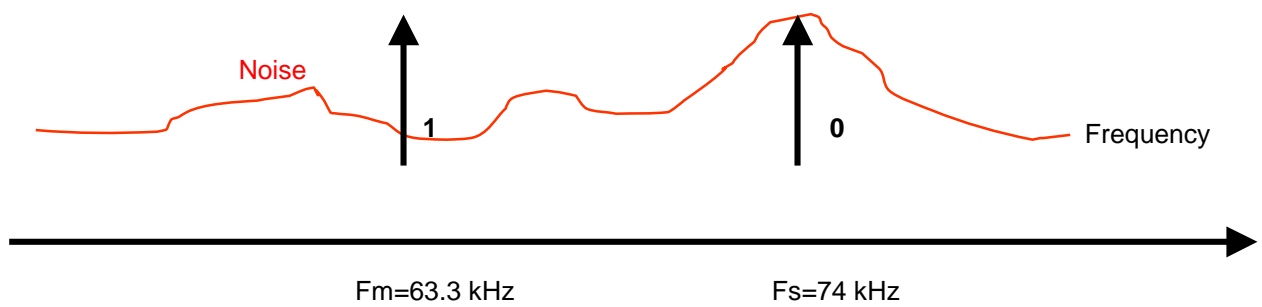
- Alarm signal during a pause
- RepeaterCall algorithm for auto-adjustment of the Repeater state

### 2.2.1 Modulation/demodulation description

The modulator/demodulator characteristics are as follows:

- Modulation: S-FSK (Spread-Frequency Shift Keying)
- Communication frequencies:
  - Fm (Mark frequency - Mark): 63.3 kHz
  - Fs: (Space frequency - Space): 74 kHz
- Modulation rate: 2400 Baud
- Physical synchronisation with the 50 Hz electrical network frequency

**Spread-FSK modulation: IEC 61334 – SFSK profile**



The sender assigns the  $F_s$  frequency to data "0" and the  $F_m$  frequency to data "1". The  $F_s$  and  $F_m$  frequencies are separated from one another (spread). By moving the  $F_s$  signal away from the  $F_m$  signal, the quality of their respective transmissions becomes independent of the narrow-band interference often found on the network.

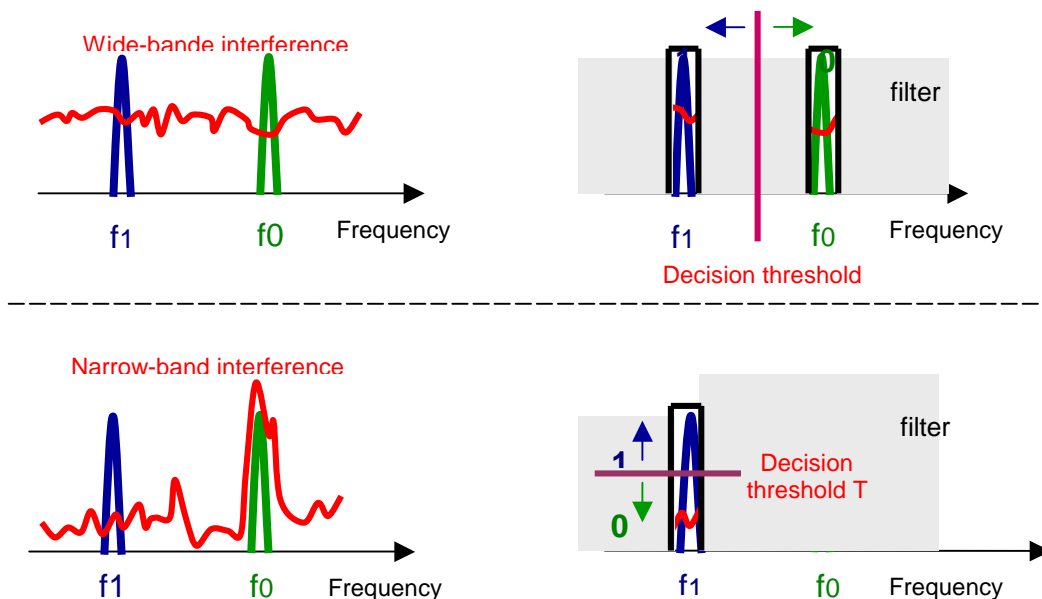
The receiver performs conventional FSK demodulation at the two possible frequencies (half-channels), which generates two demodulated signals,  $d_S$  and  $d_M$ . If the average reception quality (signal/noise ratio) of the half-channels is similar (see the figure below), the decision unit selects the higher demodulated channel ("data 0" if  $d_S > d_M$ , "data 1" if  $d_S < d_M$ ). In this case, the operating mode is FSK.

If the average reception quality of one of the two half-channels is better than that of the other, the decision unit compares the demodulated signal of the better channel with a threshold  $T$  and ignores the other channel.

The operating mode on this channel is then ASK (Amplitude Shift Keying).

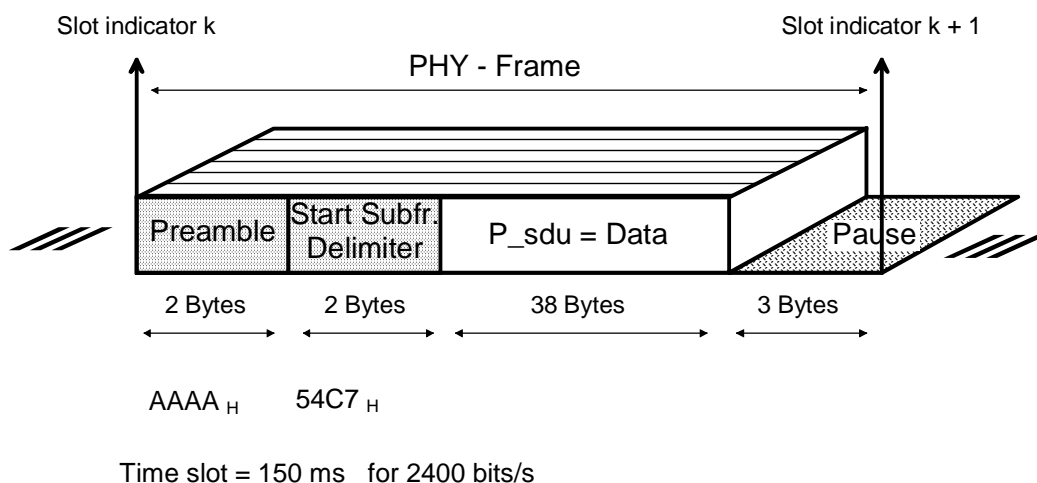
S-FSK modulation is a reliable modulation against narrow-band interference. It allows data to be transmitted even when one of the two frequencies is completely hidden by the noise on the electrical network.

The S-FSK demodulation block diagram is shown in the following figure:



### 2.2.2 Signal and noise level measurement

The frame structure is as follows:



It consists of a preamble (AAAAh), a start frame delimiter (54C7h) and 38 data bytes. Each subframe is followed by a three-byte pause that will be used to receive or send alarms.

The signal and noise are measured on the preamble and frame delimiter:

- The module fixes its receiving gain (amplification of the signal received)
- The module measures the signal and noise level at each frequency.

- S0 = reception level at Fs, when "0" is received
- N0 = reception level at Fs, when "1" is received
- S1 = reception level at Fm, when "1" is received
- N1 = reception level at Fm, when "0" is received
- The module determines the demodulation method (FSK, ASK0, ASK1)

### 2.2.3 Physical synchronisation

All the communication modules are synchronised on the "Slot Indicators" that represent the beginning of each frame.

The beginning of a frame for a Client always occurs at the zero crossing of the 50 Hz signal.

Modules connected to different phases can be synchronised because the time between the zero crossings on two different phases corresponds to a bit integer. Therefore, the Slot Indicator will always correspond to the beginning of a bit for modules connected to two different phases.

(for example, at 50 Hz and 2400 Baud: number of bits between the zero crossing of two different phases =  $1/50 * 1/3 * 2400 = 16$  bits)

At 2400 Baud, the duration of a subframe is not a multiple of 20 ms (150 ms = 7.5 x 20 ms). Consequently, the Slot Indicators are not always on a rising edge, but alternatively on a rising edge and a falling edge of the 50 Hz signal. This generates a 180° uncertainty in the delta-phase measurement, which is calculated by measuring the time between the beginning of the TSlot and the rising edge of the 50 Hz zero crossing. To eliminate the uncertainty, a Client always begins a new communication on a Timeslot corresponding to a 50 Hz rising edge. The Server receiving the frame can therefore calculate the exact value of the delta phase (correction of the 180° uncertainty) according to the frame parameters.

## 2.3 Link layer

The link layer is divided into two sublayers:

- the MAC (Medium Access Control) sublayer
- the LLC (Logical Link Control) sublayer.

The main role of the MAC sublayer is to control access to the physical layer and the physical addressing of the various PLC communication modules.

The main role of the LLC sublayer is to control access to the MAC layer and the addressing of the various applications.

### 2.3.1 MAC layer

The MAC sublayer conforms to the following standardisation documents:

- IEC 61334-5-1 [7]: determines the rules and performances expected from an S-FSK modulator/demodulator.

The MAC sublayer must implement the services specified in the extension to the standard (see [7])

- Synchronisation of PLC Modules on a Concentrator (Search Initiator). This service is described in section 2.3.2 Description of the Search Initiator function on the MAC layer of the Server

All the communication modules are addressed on the PLC network by a MAC address. The concentrator also has its own MAC address (initiator MAC address).

The concentrator assigns MAC addresses to all the modules during the discovery phase when it searches for new devices connected to the network.

Important: the MAC addresses must be assigned by the concentrator in ascending order starting with 1. This is required by the RepeaterCall mechanism (see 2.4.4.2 RepeaterCall Service).

The MAC sublayer also defines the addresses used to define the groups of PLC modules (or the groups of PLC meters).

These group addresses are used to send commands in broadcast mode (Broadcast or Multicast).

The sublayer includes the tools required to manage the repetition algorithm. This algorithm is used to forward information, even over very long distances between the concentrator and the furthest PLC module on the network. This algorithm is called "repetition with credits" (see section 4.5 Credit management).

### 2.3.2 Description of the Search Initiator function on the MAC layer of the Server

This function is an extension to IEC 61334-5-1 [7] and is compatible with this standard. The Search Initiator (Smart Synchronisation) function applies to synchronisation on a concentrator. It makes it possible not to synchronise immediately with the first frame received, but to wait for a moment in order to listen for all the concentrators present on the network and synchronise with the concentrator that is most clearly heard.

This is useful in the event of significant crosstalk, because synchronisation with the nearest concentrator will then be ensured.

"Fast" synchronisation is possible when the module hears a very strong signal.

In this case, synchronisation is immediate. This is the case with a module connected to the same point as a concentrator or to the same point as another module that has already been registered or bound to a concentrator.

### **Concentrator synchronisation search phase**

(See section 3.2 PLC and Timeout states, for a description of the states and timeouts mentioned)

When a module is not registered or bound to a concentrator (NEW and UNLOCK), it is searching for a concentrator.

During this phase, the module can synchronise with any concentrator. However, instead of remaining physically synchronised to this window, it then immediately falls physically out of sync, in order to listen for other potential concentrators.

It can then list the concentrators it hears, together with the frame reception signal level of each concentrator.

Two smart synchronisation identification parameters can be defined:

- The Time Out Search Initiator (10 minutes by default), which defines the time during which the module listens to the network in order to find all the concentrators. A value of "0" deactivates the smart synchronisation function.
- The Gain Search Initiator, which defines the maximum gain for which fast synchronisation is accepted (see 2.2.2 for how to determine the demodulation gain).

When the "TO Search Initiator" expires, the module automatically binds itself to the concentrator with the best signal level it has heard (changes to NEW and LOCK).

If the module hears a concentrator with a gain that is less than the Gain Search Initiator (very strong signal) before this timeout expires, it automatically binds itself to this concentrator (changes to NEW and LOCK) and waits to be registered.

The module does not have to be physically synchronised to be able to bind itself to a concentrator.

### **Concentrator registration pending phase**

Once the module is bound to a concentrator (NEW and LOCK), it waits to receive a Register frame (from the correct concentrator) with its serial number to enable it to change to the registered state (Not NEW and LOCK).

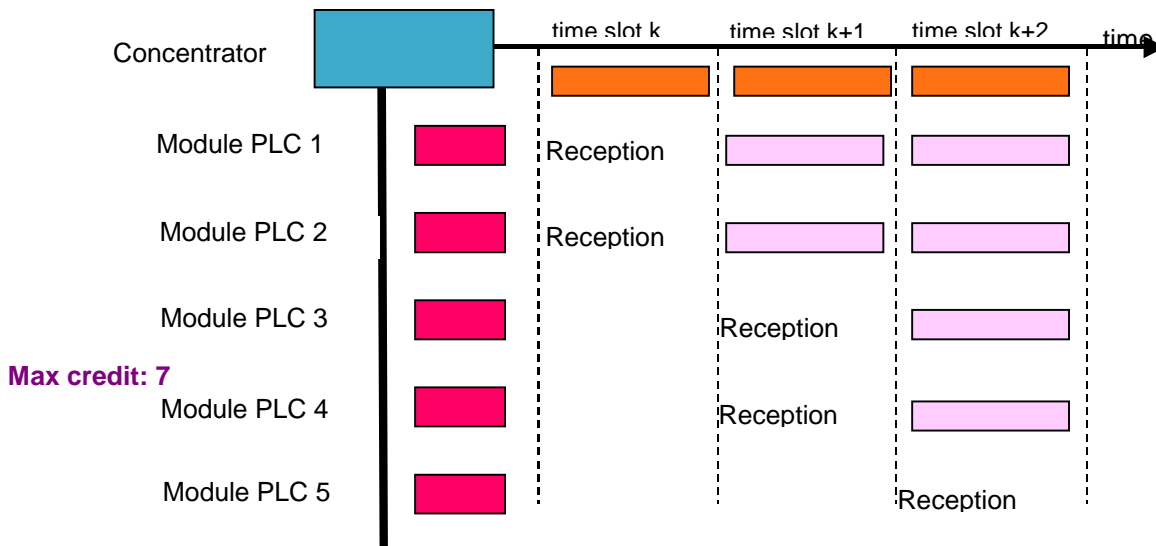
If the module does not receive a Register frame from the concentrator, it returns to the synchronisation search phase (NEW and UNLOCK) when "TO not Addressed" expires (6 hours by default).

If the module does not receive a correct frame (CRC Ok) from the concentrator when the "TO Search Initiator" expires, it returns to the synchronisation search phase (NEW and UNLOCK).

### **2.3.3 Description of the MAC layer for repeating a frame consisting of a subframe**

The PLC Module uses the MAC sublayer resources to manage message repetition on the network. Credit management is described in section 4.5, Credit management, and is illustrated in the following example:

## Linky PLC profile functional specifications



All the PLC modules and the concentrator are synchronised to the 50 Hz signal. The time is divided into time-based windows called time slots.

All the frames are transmitted synchronously with the 50 Hz signal and the beginning of the time slot.

In the example in the figure shown above:

- The concentrator sends a frame (addressed to PLC module 5) with a repetition credit of 2 during time slot k.
- PLC modules 1 and 2 receive and understand the frame. However, the transmission conditions are too bad (impedance too high, distance too long) for PLC modules 3, 4 and 5 and they cannot receive the message correctly.
- The concentrator and PLC modules 1 and 2 repeat the same frame, at the same time, with a repetition credit = 1 (the credit has been decremented by 1) during the next time slot (k+1).
- PLC modules 3 and 4 receive and understand the frame. The distance is too long for PLC module 5 and it does not receive the message.
- The concentrator and PLC modules 1, 2, 3 and 4 repeat the same frame, at the same time, with a repetition credit = 0 (the credit has been decremented by 1) during the next time slot (k+2).
- PLC module 5 receives and understands the frame.

The maximum repetition credit is 7. Although the maximum distance for a direct communication is approximately 300 m, the repetition algorithm can be used to reach devices located at a maximum distance of 2400 m (300 m x 8) from the concentrator.

With this repetition principle, the PLC system does not require the repetition "routing" table to be programmed. The best communication path is automatically found on the network. It automatically adjusts to the transmission conditions (interference, change of impedance on the network, etc.).

The concentrator automatically and continuously adjusts the value of the credit used for each PLC module in order to optimise communication times. (See section 4.5 Credit management).



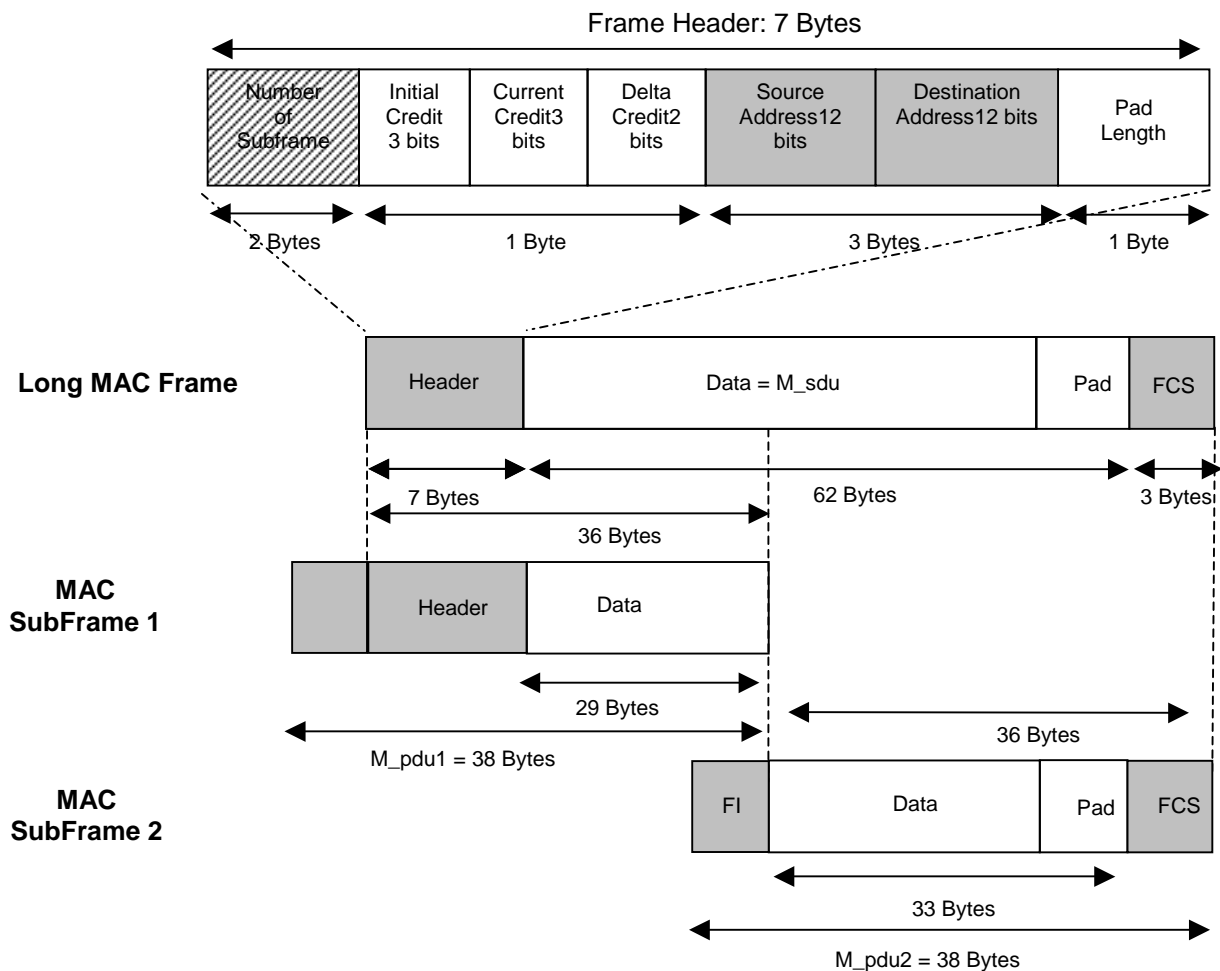
## Linky PLC profile functional specifications

- Padding byte field
- Frame control sequence (FCS): 3 bytes.

A cyclic redundancy code (CRC) is used to generate the frame control sequence, known as FCS (see [A1], section 4.3).

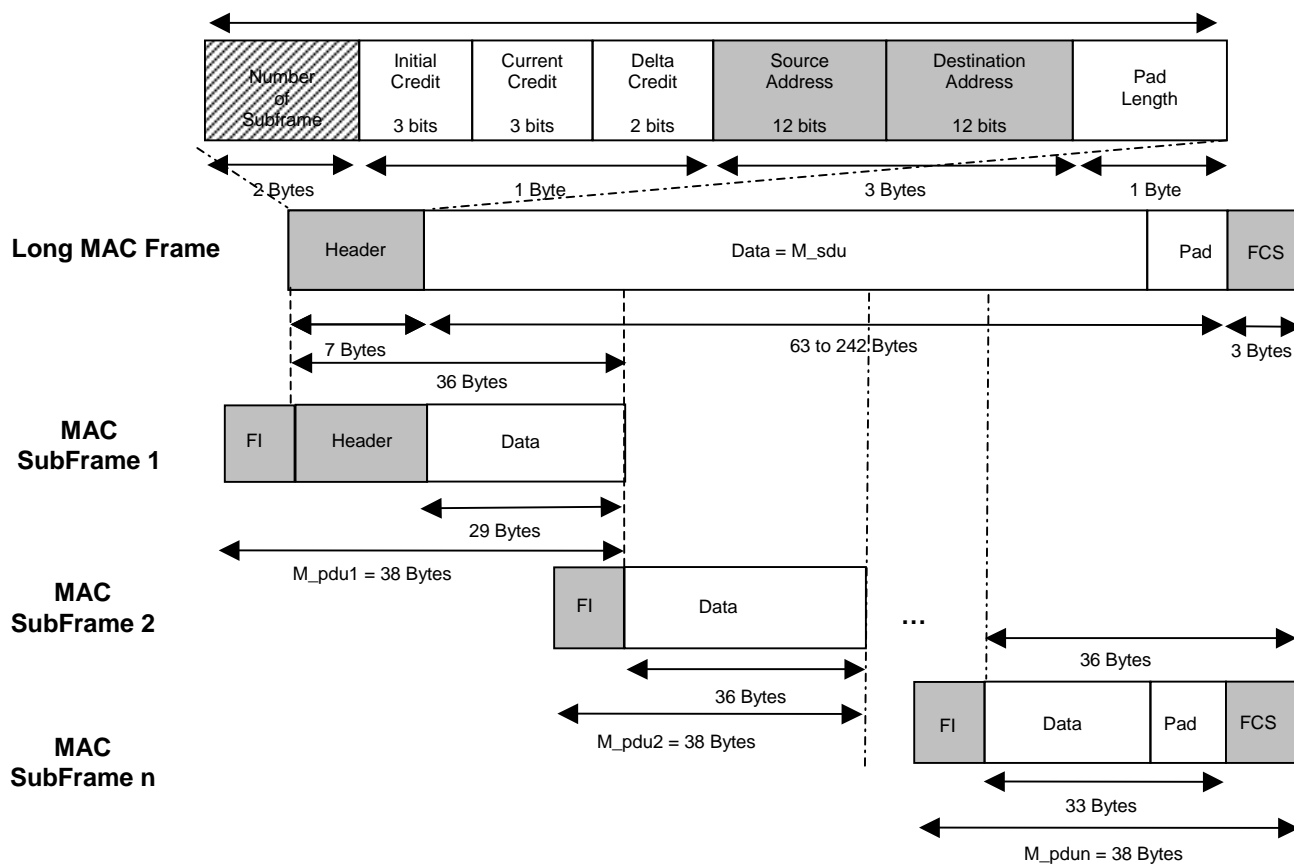
### 2.3.5 Description of the MAC layer for a frame consisting of two subframes

Frame structure with two subframes:



2.3.6 Description of the MAC layer for a frame consisting of n subframes

Frame structure with n subframes:



The maximum length of data that can be carried in a MAC layer frame is 242 bytes.

### 2.3.7 LLC layer

The LLC sublayer is as specified in IEC 61334-4-32[2].

## 2.4 Application layer

The application layer is located directly above the LLC sub-layer.

The following two different application protocols are implemented, according to the Server profiles:

- DLMS, as described in the standardisation documents [3],
- COSEM, as described in the standardisation documents [13] [14].

To manage the PLC network, the application layer uses [5].

### 2.4.1 DLMS Application layer

From the communication point of view, a "DLMS" physical device (PLC module for Yellow meter or PME/PMI meter) can be divided into several virtual entities or VDEs (Virtual Distribution Equipment). Each VDE supports all the DLMS\_ASE services defined by the DLMS application protocol.

Each VDE consists of virtual objects classed by type and accessible via specific services (variableNames).

A BCPL for managing "Yellow tariff" meters is defined by the following VDEs:

- Management VDE, which defines all the objects associated with the management of the PLC network [5][6]
- Euridis meter VDE, which manages the Euridis meters (for example the "Yellow tariff" meter) (see [A2])

A BCPL that controls the "PME/PMI" meters is defined by the following VDEs:

- Management VDE, which defines all the objects associated with the management of the PLC network [5][6],
- VDEs specific to the PME/PMI meter (see [A3])

The encoding rules are described in the A-XDR standardisation document [11].

## 2.4.2 COSEM application layer

### 2.4.2.1 General

From the communication point of view, a "COSEM" physical device (Linky meter) can be divided into several virtual entities or Logical Devices. Each Logical Device supports all the xDLMS\_ASE services defined by the COSEM application protocol. At least the standard DLMS services defined by this application protocol for ShortName referencing will be supported.

Each logical device consists of virtual objects (class instances) classed by type and accessible via specific services (class methods or attributes, referenced by ShortNames).

The Linky meter consists only of a single Logical Device and this choice optimises communication during the connection phases.

PLC Linky meter modelling is described in section 2.1.2 Reference model for the Linky meter.

The objects associated with PLC network management are defined by the COSEM ID 50, 51, 52, 53, 56 Class instances described in the Blue Book [13].

The encoding rules are described in the A-XDR standardisation document [11].

The objects accessed via the COSEM application layer are identified according to the rules specified in IEC 62056-61 [9] (OBIS code).

The objects associated with PLC network management are defined by COSEM class instances (section 2.4.3).

### 2.4.2.2 New functions

The application layer is used to send data from the APDU by Data Blocks, in read or write mode.

(See Green Book [14])

## 2.4.3 Correspondence between the MIB and COSEM classes for the PLC

### 2.4.3.1 Correspondence between the MIB objects and the PLC classes

MIB object in conformance with IEC 61334-4-512 [6]	COSEM class instances	Attribute name	Attribute no.
delta-electrical-phase	PLCPhysicalSetup	delta_electrical_phase	3
max-receiving-gain	PLCPhysicalSetup	max_receiving_gain	4
mac-address	PLCPhysicalSetup	mac_address	8
mac-group-addresses	PLCPhysicalSetup	mac_group_addresses	9
Repeater	PLCPhysicalSetup	repeater	10
	PLCPhysicalSetup	repeater_status	11
synchronisation-confirmation-time-out	PLCSynchTimeOut	synchronization_confirmation_timeout	3
time-out-not-addressed	PLCSynchTimeOut	timeout_not_addressed	4
time-out-frame-not-ok	PLCSynchTimeOut	timeout_frame_not_OK	5
min-delta-credit	PLCPhysicalSetup	min_delta_credit	12
synchronisation-locked	PLCPhysicalSetup	synchronization_locked	14
reply-status-list	PLCLogicalLinkControlSetup	reply_status_list	3
L-SAP-list	SapAssignment	SAP_assignment_list	2
active-initiator	PLCActiveInitiator	active_initiator	2
reporting-system-list	PLCReportingSystemList	reporting_system_list	2
reset-NEW-not-synchronised	PLCActiveInitiator	reset_NEW_not_synchronized	129
initiator-electrical-phase	PLCPhysicalSetup	initiator_electrical_phase	2

## Linky PLC profile functional specifications

broadcast-frames-counter	PLCMacCounter	broadcast_frames_counter	4
repetitions-counter	PLCMacCounter	repetitions_counter	5
transmissions-counter	PLCMacCounter	transmissions_counter	6
CRC-Okframes-counter	PLCMacCounter	CRC_OK_frames_counter	7
synchronisation-register	PLCMacCounter	synchronization_register	2
desynchronisation-listing	PLCMacCounter	desynchronization_listing	3
application-context-list	Not applicable		
broadcast-list	Not applicable		

The objects described in the MIB and not processed in COSEM are not used in the BCPLs, the PME/PMI meters or the Linky meters.

S-FSK Reporting system list (class\_id: 56) is not used in the Linky project.

### Special repeater status case:

The repeater status is described as a single object in the MIB, but seen as two different attributes of the PLCPhysicalSetup instance in COSEM. The correspondence between the *repeater* variable values in MIB and the *repeater* and *repeater\_status* variables in COSEM is described below.

MIB		COSEM		
<i>repeater</i>		<i>repeater</i>		<i>repeater_status</i>
Always	1	Always	1	TRUE
Never	0	Never	0	FALSE
Repeater ISAcalls	3	Dynamic	2	TRUE
NoRepeater ISAcalls	2	Dynamic	2	FALSE

### 2.4.3.2 MIB objects not described in IEC 61334-4-512 [6]

The table below lists the MIB objects added to the COSEM PLCPhysicalSetup, PLCMacCounter, PLCLogicalLinkControlSetup and PLCSynchTimeOut classes not described in IEC 61334-4-512 [6]. The description of these objects that can be accessed by the management application via the MIB will be added to the particular specifications of the PLC modules for the yellow tariff and PME/PMI meters.

COSEM class	NonAttribute	Attribute no.
PLCPhysicalSetup	max_transmitting_gain	5
PLCPhysicalSetup	search_initiator_gain	6
PLCPhysicalSetup	frequencies	7
PLCMacCounter	CRC_NOK_frames_counter	8
PLCPhysicalSetup	initiator_mac_address	13
PLCLogicalLinkControlSetup	max_frame_length	2
PLCSynchTimeOut	search_initiator_timeout	2

### 2.4.4 CIASE

The discovery and registration functions of the new PLC modules are implemented via the services defined in IEC 61334-4-511: CIASE [5].

The CIASE services used (Protocol Configuration Initiation Application Service Element) are as follows:

- Discover
- DiscoverReport
- Register
- PingService (CIASE standard functional extension [5])
- RepeaterCall (CIASE standard functional extension [5])
- ClearAlarm (CIASE standard functional extension [5])

CIASE is an application protocol in non-connected mode.

The role of the new functions is described below, but the way in which they are used is described in [A1].

### **2.4.4.1 Ping service**

#### 2.4.4.1.1 Purpose

The Ping service allows a confirmed request to be sent in point-to-point (non-connected) mode. This service will be used to check that a Server system is always present on the network and to maintain the "To Not Addressed" object on each PLC module.

#### 2.4.4.1.2 Principle

When a Client system does not have a specific task to perform, it runs a background task to maintain the state of the network. This background task involves sending a Ping request to each module in turn. The purpose of this background task is to:

- reset the Timeout not addressed object on each module
- check that each MAC address corresponds to the correct Server system (avoids "duplicates")

A duplicate is a module that has the same MAC address as another module.

### **2.4.4.2 RepeaterCall Service**

#### 2.4.4.2.1 Purpose

The RepeaterCall service is used to adjust the repeater status of a PLC module according to the topology of the electrical network.

The RepeaterCall service is the CIASE service that automatically configures the repeater status of the entire network.

#### 2.4.4.2.2 Principle

When requested by the Client system, all the Server systems on the network enter the RepeaterCall mode. In this mode, each module sends a signal in turn.

If several modules are nearby, the signal sent by one of the modules will be heard by the others. One of these modules will be the repeater for the whole group. Conversely, if the modules are far apart, they will not hear the signal sent by other modules and it will automatically be repeater.

### **2.4.4.3 ClearAlarm service**

#### 2.4.4.3.1 Purpose

The ClearAlarm service allows the Client system to remove alarm information from one or more Server systems.

#### 2.4.4.3.2 Principle

After reading the pending alarm message on one or several modules, the Client system must send a request to clear the alarm in question from these modules. This request can be sent in point-to-point or broadcast mode and makes it possible to clear a specific alarm bit from the Client systems addressed.

## **2.4.5 Alarm management**

Alarms allow a Server to inform a Client at any time that it has information to send to it. After notifying this alarm, the Client determines which Server is in the alarm state in order to query it and control the alarm state.

(See the description of the alarms in [A1]).

### 2.4.5.1 Server side

When a server detects an alarm, it informs the Client via the phy.alarm.request service (CIASE protocol, see section 2.4.4 CIASE).

A Server can control 32 alarms. Two 32-bit registers are used to control the alarms:

- AlarmRegister (32 bits, R/W): register containing the state of the alarms. Each bit corresponds to an alarm and a bit value of 1 corresponds to a detected alarm. Writing a bit in this register clears this bit. The "Write.request" or "ClearAlarm" service (CIASE protocol) clears one or more bits from this register.
- AlarmFilter (32 bits, R/W): register used to deactivate the alarms individually (a bit value of 0 deactivates the corresponding alarm).

When an alarm is detected, the corresponding bit in the AlarmRegister will be set to 1 only if the alarm is activated: corresponding bit value of 1 in AlarmFilter.

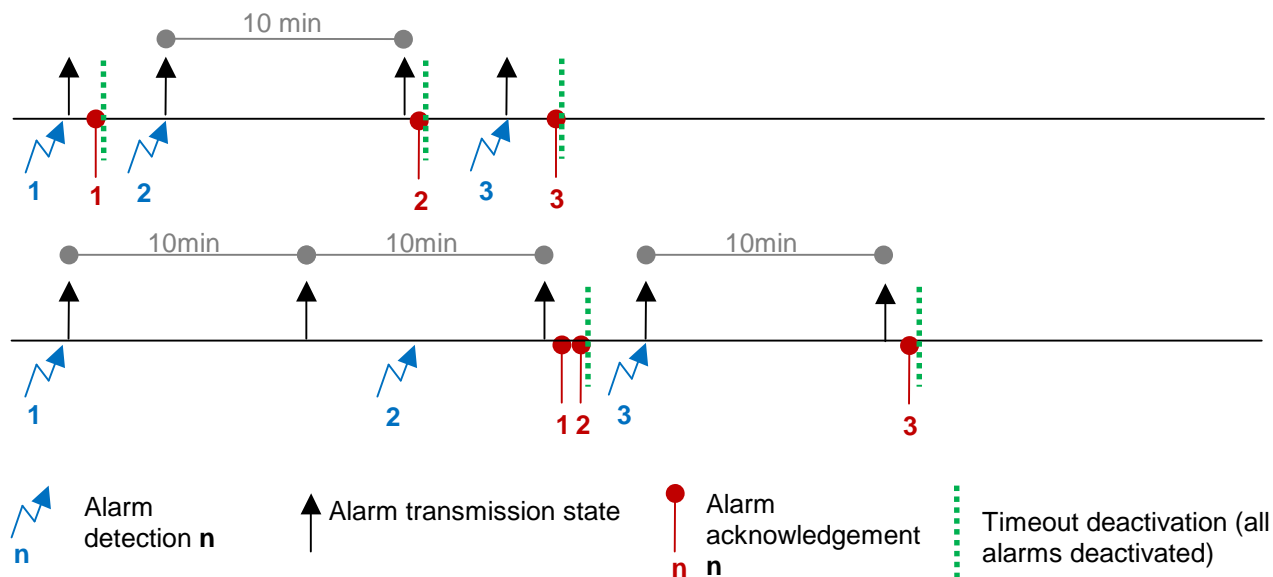
Special case: bit 0 in the AlarmRegister corresponds to a Server NEW state notification. This bit cannot be cleared by the "ClearAlarm" service. It is cleared automatically after the "Register" service (CIASE protocol), when the Server is no longer in the NEW state.

#### Sending an alarm state to the Client

A server sends an alarm state via the phy.alarm.request service (CIASE protocol) if at least one bit in the AlarmRegister has a value of 1. As long as all the alarms on this server are not acknowledged by the Client, the alarm state will be transmitted cyclically.

When the alarm state has been sent, the TO\_Alarm\_Repeat Timeout is triggered: the alarm state will be returned when this timeout expires, if at least one alarm is not acknowledged.

If a new alarm is detected while this Timeout is activated, the alarm state will not be sent immediately, but when this Timeout expires. If all the alarms are acknowledged, the Timeout is deactivated.

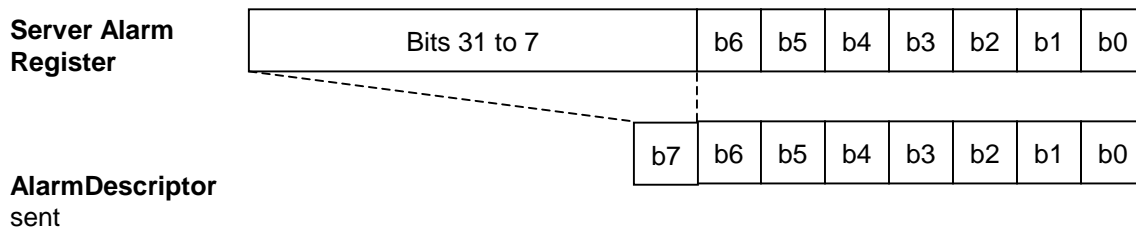


### 2.4.5.2 Client side

The client waits for a "phy.alarm.indication" from the physical layer, which indicates that at least one Server has detected an alarm. The Client then initiates an alarm retrieval procedure on the servers.

### Alarm retrieval procedure

After receiving an alarm indication, the Client initiates a network discovery procedure: Discover.Request service (CIASE protocol) addressing all the servers: All\_physical\_address (0xFFFF). The servers with an alarm to be notified respond with the DiscoverReport service (CIASE protocol) containing their serial number and an "AlarmDescriptor" byte. This byte indicates the current alarm type:



- Bits 0 to 6 of the AlarmDescriptor are the same as bits 0 to 6 in the Server AlarmRegister. If one of these bits is read as 1, the type of alarm notified is immediately known.
- AlarmDescriptor bit 7 includes AlarmRegister bits 7 to 31: when at least one of these bits has a value of 1, the value of bit 7 in the AlarmDescriptor is 1.

To retrieve the alarms, two cases are possible, depending on the AlarmDescriptor value:

- If bit 7 has a value of 0, the notified alarms are stored directly in this byte with the Server serial number received when the Report was issued.
- If bit 7 has a value of 1, the Server must be queried by reading the AlarmRegister (this register can be accessed in Read mode by the Public Client) and the alarms in the response stored.

The stored alarms must then be removed by the "ClearAlarm" service (CIASE protocol), apart from the alarm corresponding to the AlarmRegister bit 0, which indicates the NEW state (it is cleared after the CIASE protocol "Register" service).

At the end of this procedure, the "TO\_Alarm\_management" Timeout is triggered. During this Timeout, the alarm indications are filtered and saved: if an alarm indication is received before the end of this Timeout, the alarm retrieval procedure will only be triggered when the Timeout has expired. The value of this Timeout is a concentrator parameter. By default, its value (0) is used to notify the alarms in real time.

#### 2.4.5.3 Network discovery

This alarm mechanism is used to speed up the discovery of a new PLC module on the network.

In fact, this mechanism is used by a newly installed meter to notify the concentrator that it must start a discovery phase.

The meter can then very quickly be discovered, without waiting for the regular concentrator discovery cycle.

### **3. PLC FUNCTIONS ASSOCIATED WITH A METER**

#### **3.1 Physical synchronisation**

When the PLC module is first powered up, it locks its PLL (synchronises its clock to the 50 Hz signal) and waits for a Physical synchronisation (TSlot).

The PLC module is in the "NEW and UNLOCK" state, because it has never been registered by a concentrator. It has no MAC address on the PLC network and is waiting to be registered.

A PLC module is physically synchronised (to the electrical network) when it has found a window or time slot. A window lasts 150 ms (duration of a subframe) and begins at a zero crossing (the voltage goes to 0 at 50 Hz).

When a device is physically synchronised, it can only receive the frames sent by other devices with the same physical synchronisation, i.e. usually by one concentrator (since the concentrators are not synchronised).

When a device is physically desynchronised, it searches for a physical synchronisation. It is physically synchronised as soon as it finds an "AAAA" pattern followed by the "54C7" start delimiter corresponding to the beginning of a subframe (see 2.2.1 Modulation/demodulation description).

Synchronisation occurs when the first PLC frame is seen on the network (inactive smart synchronisation).

It can also be synchronised more "smartly" in order to improve system operation in the event of significant crosstalk between adjacent PLC networks (see section 4.8 Crosstalk management).

During the concentrator discovery process (see 2.3.2 Description of the Search Initiator function on the MAC layer of the Server), the PLC module in the NEW state sends its "serial number" ADS identifier. The concentrator registers the PLC module (the latter changes from the NEW state to the REGISTERED state) and assigns it a local MAC address.

In the REGISTERED state, the PLC module has a MAC address and is locked onto a concentrator (locked onto an initiator MAC address).

It can then be accessed by a concentrator and therefore by the IS.

## 3.2 PLC and Timeout states

### 3.2.1 PLC states

#### **Synchronised state:**

The PLC module is physically synchronised to a frame received from a concentrator.

#### **NEW and UNLOCK state:**

Any concentrator can register a PLC module in this state. The PLC module has no MAC address and cannot communicate with a concentrator.

#### **NEW and LOCKED state:**

Only the concentrator already known by the PLC module can reregister it. An Initiator address is stored by the PLC module (the Initiator MAC address used during the registration phase).

#### **REGISTERED state:**

The PLC module has a MAC address and is locked onto a concentrator (Initiator MAC address).

### 3.2.2 Timeouts

#### **Time out confirmation:**

When a PLC module is not physically synchronised and synchronises to an "AAAA54C7" pattern, a time equal to "Time out confirm" is activated until the module receives a correct frame (CrcOk). When this timeout expires, the module returns to the physical synchronisation search mode. However, during the timeout, as soon as a correct frame is received, this timeout is cleared.

The default value is 30 s.

#### **Time out not ok:**

When a PLC module is physically synchronised, if no other correct frame (CRC invalid, frame not received) is transmitted over the network for a time equal to "Time out not ok", the PLC module loses its physical synchronisation and waits for a new one.

The default value is 40 s.

#### **Time out Search Initiator:**

When a PLC module in the NEW and UNLOCK state wants to search for the concentrator with the strongest transmission signal on this part of the network, this Timeout must be greater than 0. Otherwise, the search for the best concentrator is not activated and the module will be synchronised with the first concentrator it hears.

In the case of a module in the NEW and UNLOCK state, this timeout is activated as soon as a frame is received. When this timeout has expired, the module will physically synchronise only with the concentrator with the greatest signal/noise ratio measured earlier.

The default value is 10 minutes.

#### **Time out not addressed:**

When a PLC module is REGISTERED, it is locked onto its concentrator (Initiator MAC address). If it does not receive a frame during a time equal to "Time out not addressed", the PLC module changes from the REGISTERED state to the "NEW and UNLOCK" state.

The PLC module now waits to be registered by any concentrator.

The default value is 6 hours.

### **3.2.3 State changes**

#### **Changing the timeout states**

If a registered module (not NEW) does not receive any correct frames during a time period between "Time out not ok" (40 s) and "Time out not addressed" (6 h), the module remains in its registered state (Not NEW). It waits to be physically synchronised if no correct frame (CRCok) is received during this time period.

If it has not received any correct frames addressed to it after "Time out not addressed" (6 h), it changes to the NEW and UNLOCK state.

#### **Replacing a meter on a BCPL**

When a new meter is installed on a registered PLC module, it changes from the "REGISTERED" state to the "NEW and LOCKED" state.

It will be rediscovered by the same concentrator and will send information from the new meter (serial number).

#### **Changing the concentrator (new Initiator MAC address):**

All the registered PLC modules change from the "REGISTERED" state to the "NEW and UNLOCK" state after a time equal to "Time out not addressed".

The new concentrator can then discover and register them.

## 4. PLC FUNCTIONS ASSOCIATED WITH A CONCENTRATOR

### 4.1 Management of PLC communication modules

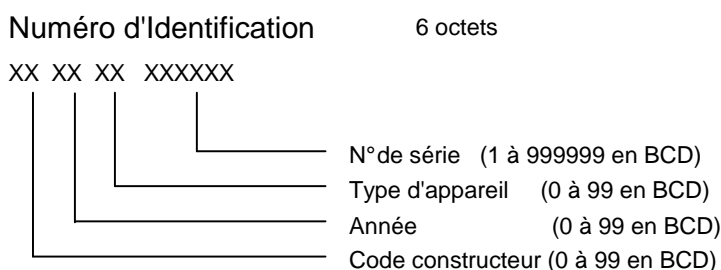
The discovery and registration functions of the new PLC modules are implemented via the CIASE services [5].

The concentrator supports various application contexts. Within the framework of the Linky project, this application context is associated with the following characteristics:

- Transfer syntax: A-XDR (specification of the rules for encoding and decoding values defined by ASN.1 for DLMS PDUs)
- Crypted or non crypted mode

### 4.2 Equipment identification

The identification structure of all the PLC network devices, including that of the concentrator (Euridis type identifier) is as follows:



In this document, the Euridis identifier is often called the serial number, the identification number or the system title.

### 4.3 Discovery function

Various types of communication modules are managed by the concentrator:

- Modules integrated with the electronic meter (single-phase and three-phase Linky meters)
- Independent modules with a Euridis interface (for example PLC modules for the Yellow tariff CJE meter)
- Independent modules with a serial/DLMS interface (for example PLC modules for the PME/PMI type meter).

The concentrator uses the CIASE application protocol services (see section 2.4.4 CIASE) to detect and register the new PLC communication modules. This function is ensured by the "System management" application process (see section 2.1.1 Reference model for the Linky concentrator).

The process used to discover and register the new PLC communication modules has three communication elements:

- **"NEW"**: state of a module that is not registered and that can only be addressed by the MAC address "All\_physical\_address" or by the "New\_Address".  
In some cases, a module in the "NEW" state can be pre-bound to a defined Initiator MAC address; this means that it will only respond to requests from the concentrator that has this address.
- **"REGISTERED"**: state of a registered module, i.e. it has been assigned an individual MAC address by the concentrator.

- **"INITIATOR"**: the initiator is the concentrator. It initiates the new module registration procedure.

#### 4.4 Description of the registration process

##### 4.4.1 For a new module (Server)

The registration process is fully "plug and play".

The MAC address of a newly installed module or a module that has been initialised following a change in its operating context is set to "New\_Address".

The module knows its own identification number (unique Euridis identifier).

The concentrator sends **Discover** type messages (calling PLC modules in the "NEW" or alarm states) at regular intervals (the frequency can be programmed).

For its part, the module waits for this **Discover.request** primitive and the associated A\_pdu. This **discover.request** A\_pdu is sent with the destination MAC address: "All\_physical\_address" and the destination LSAP address: **"System Management"** Server (CIASE).

It contains the various discovery management parameters described in the CIASE document.[5]:

- Initiator MAC address
- The number of Time Slots allocated for the Reports.
- The "Response probability" parameter, which defines the probability (as a percentage) of a PLC in the NEW state responding to the Discover request. When this parameter is 100, all the modules in the NEW state will respond.

The "NEW" module selects a time slot at random and sends a DiscoverReport containing its identification number.

The concentrator sends a Register frame with the MAC destination address: "All\_physical\_address" and the destination LSAP address: "Management".

This command contains the list of the identifications of all the newly discovered modules and the list of the MAC addresses assigned by the concentrator.

If the module recognises its own identification number, it changes from the "NEW" initial state to the "REGISTERED" state.

From now on, the module can be queried by the concentrator because it has its own individual MAC address.

**Note:** a module that receives no requests specifically addressed to it within a defined period of time (Timeout\_not\_addressed) returns to the "NEW" and "UNLOCK" state (not registered and not bound to a concentrator).

##### 4.4.2 For the concentrator (INITIATOR)

A newly commissioned concentrator has no network image in its database, whereas a concentrator that has been operating for some time has identified all the network devices to which it is connected. The "NEW" state module search procedure must therefore be used to identify the largest number of devices during commissioning or to identify any new devices.

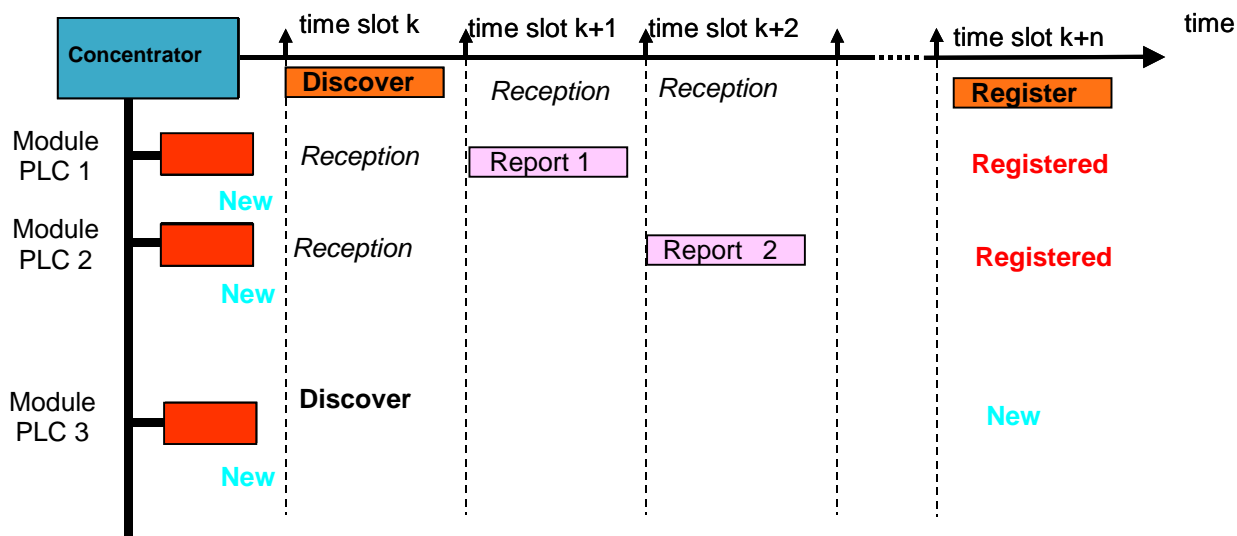
In the first case, the time taken to discover the network devices depends on the number of such devices and can therefore be significant (several minutes).

If a module does not respond within a given time period (Timeout\_not\_addressed), it is deemed to be "lost" and the concentrator stops communicating with it, causing it to change to the "NEW" state.

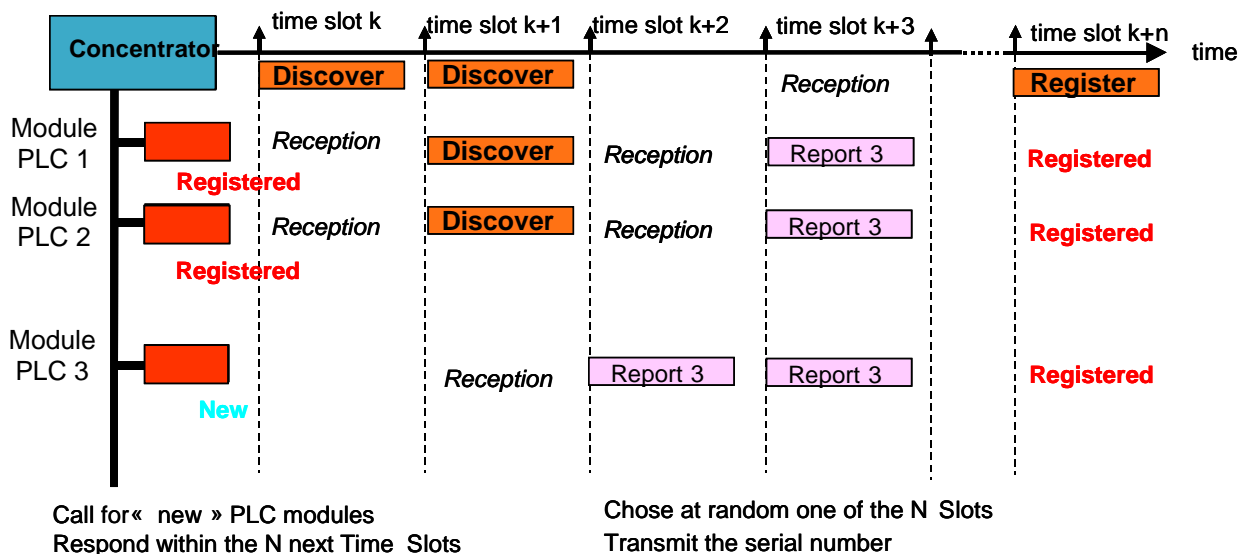
The concentrator always makes available to the IS all the modules+meters in its database, whatever their state with respect to the PLC communication.

The exchange of PLC data during a discovery and registration process performed by the concentrator is illustrated in the following figures:

**Automatic detection of new PLC modules: credit = 0**



**Automatic detection of new PLC modules: credit = 1**



When it is first started up, the concentrator sends a "Discover" discovery frame with a credit of 0.

Each PLC module in the "NEW" state, which has understood the discover request sends a report with a credit of zero.

When it has received all the reports from the PLC modules in the "NEW" state, the concentrator sends a Register frame. When the modules receive this command, they change from the NEW to the REGISTERED state.

The concentrator sends Discover commands with a credit of zero. After each Discover command, the concentrator sends a Register frame if it has received any Reports. As long as it is receiving Reports, it continues to send Discover commands with the same credit. When it does not receive any more Reports, it performs the same operation, incrementing the credit to 1, and so on, until it reaches the maximum credit that can be configured by the IS (between 0 and 7, default value = 2).

Each PLC module in the "NEW" state, which has understood the Discover Request after a registered module has been repeated, sends a report with a credit of 1.

The Report is repeated by the registered modules.

The concentrator stops the process as soon as it has no more reports and has reached the maximum credit value.

The concentrator uses this algorithm to discover automatically, in each area in turn, the PLC modules distributed over the entire distribution network (each area corresponds to the group of modules operating at the same credit value).

#### 4.5 Credit management

Credit management is a function that can be configured by the IS. It is predefined in the concentrator.

It allows the concentrator to optimise repetition credit management with all the PLC modules.

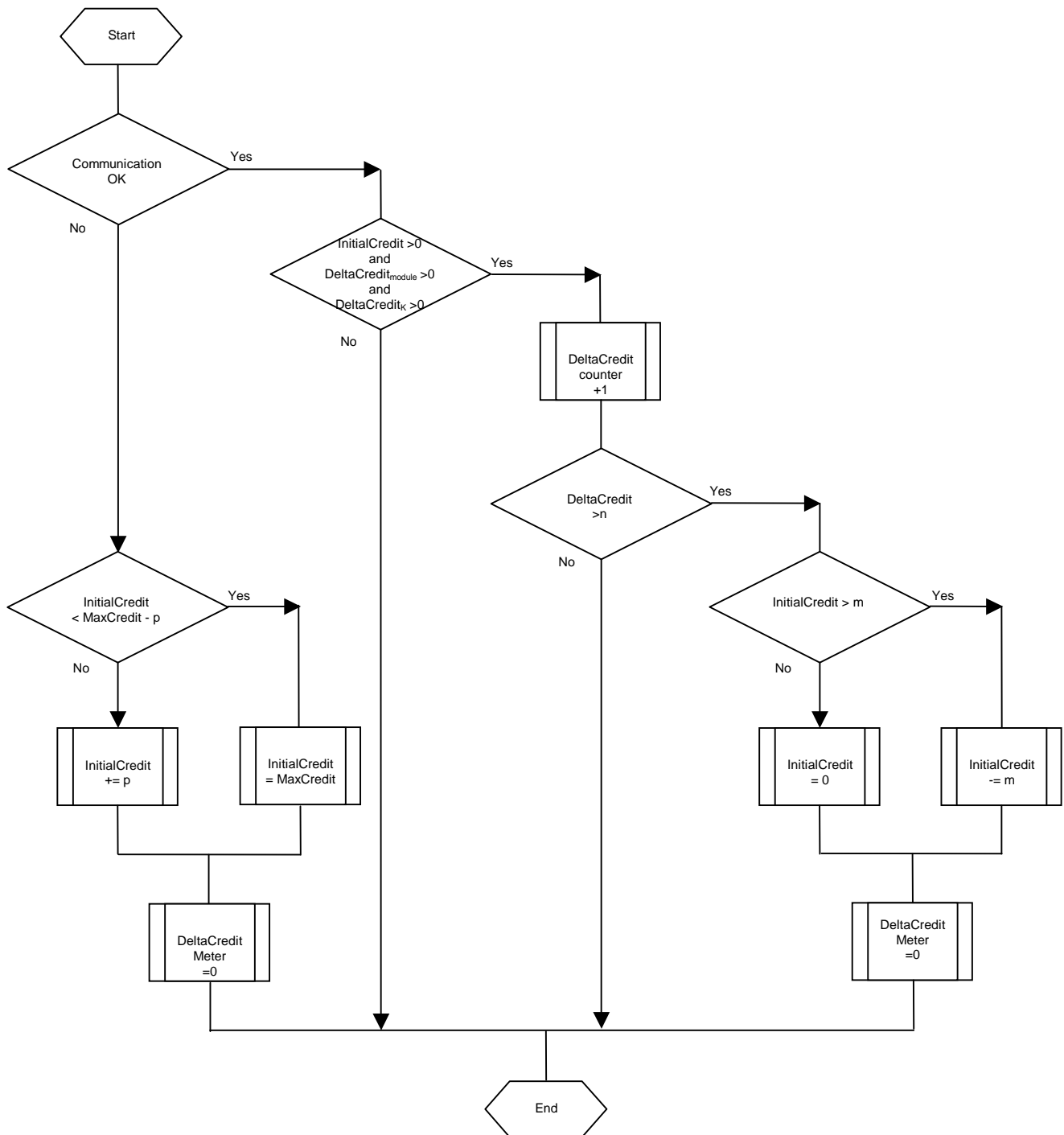
The credit management algorithm used is described below.

- The **InitialCredit** is the credit value used to exchange messages between a concentrator and a PLC module.
- The **DeltaCredit<sub>module</sub>** is the current credit value of a message sent by the concentrator when it is received by a module. This value is sent to the concentrator in the MAC response frame. The **DeltaCredit<sub>module</sub>** value can be between 0 and 3. If it is greater than 3, the **DeltaCredit<sub>module</sub> = 3**
- The **DeltaCredit<sub>CR</sub>** is the current credit value of a message sent by a module when it is received by the concentrator. This value is determined by the concentrator. The **DeltaCredit<sub>CR</sub>** value can be between 0 and 7.
- **DeltaCreditMeter** is the meter indicating the number of consecutive times that DeltaCredit and CurrentCredit were both greater than zero.
- **FlagCredit** is a Boolean value indicating the failure (True) or success (False) of the previous communication between a concentrator and a module.

The repetition credit management parameters are as follows:

- n: number of successful communications before decrementation of the initial credit. This value must be between 1 and 7. Default value: n = 1.
- m: value to be deducted from the initial credit during decrementation  $1 \leq m \leq 7$  (default value: m = 1).
- p: value to be added to the initial credit during incrementation  $1 \leq p \leq 7$  (default value: p = 2).
- q: number of tests in the event of communication failure.  $1 \leq q \leq 7$  (default value: q = 3).

These parameters can be changed in the concentrator by the IS.



#### 4.6 Calculating the Timeout between two requests

When the concentrator sends a request, a timeout is calculated to determine the time required for it to receive the response. This timeout is calculated as a number of time slots. It is calculated as follows:

For a read or write frame in point-to-point mode:

$$(Nb\_timeslot\_request * (Initial\_Credit + 1)) + (QOS) + (Nb\_timeslot\_response * (Initial\_Credit + 1))$$

For a read or write frame in broadcast mode:

$(Nb\_timeslot\_request * (Initial\_Credit + 1)) + 1$

Description of the parameters used for these calculations:

- the number of time slots in the request is calculated according to the length of the frame (between 1 and 7)
- the QOS (Quality of Service) measures the time required for the PLC module to prepare the response. It is expressed in Time Slots and is negotiated when the module is initialised.
- the number of time slots in the response is estimated according to the type of access and it always has the maximum possible value for a response with this type of access (between 1 and 7)
- the initial credit is known when the frame is sent (see previous section to calculate the initial credit)

If a PLC module takes longer than the time defined by the QOS to prepare its response, it will not send its reply.

#### **4.7 Disappearance, loss of module/meter**

After the discovery cycles, the serial numbers of the various modules/meters are stored by the concentrator. If there is no explicit request from the application software, the concentrator polls the modules on the network at regular intervals (background task) by querying a management VDE object (configurable) or the CIASE application protocol ping.request service (see section 2.4.4 CIASE).

If, at any time, the concentrator obtains no response from the module (request or background task), the module is added to the list of meters that have "disappeared". As soon as communication is reestablished with this module, it is removed from the list and will again be indicated as "accessible". A meter indicated as "disappeared" is merely inaccessible by the concentrator. It is not possible to guess the state of the module, because the reason for the communication failure is not known.

If the concentrator does not obtain a response from a module (request or background task) within a time equal to "Time out not addressed", the module is added to a list of "lost" meters.

The concentrator always makes available to the IS the list of all the modules+meters in its database, whatever their state with respect to the PLC communication ("accessible", "disappeared" or "lost").

The module remains stored in the concentrator, as long as it has not explicitly been removed by the IS.

If the concentrator discovers it again, it will assign it the same MAC address.

#### **4.8 Crosstalk management**

##### **4.8.1 Smart synchronisation**

In the most usual case, synchronisation occurs when the first PLC frame is seen on the network.

In the event of significant crosstalk between distribution stations, it is advisable to use the "smart" synchronisation function (see section 2.3.2 Description of the Search Initiator function on the MAC layer of the Server) which allows a PLC module to select the best concentrator from those it can hear.

##### **4.8.2 Repeater cluster management**

The repeater clusters positioned at the same point in the network contribute to the crosstalk phenomenon by strengthening the level of the signal transmitted.

In order to limit the impact of these clusters, the concentrator ("SystemManagement" application process) uses the CIASE application protocol "repeater call" or "automatic repeater state management" service (see section 2.4.4 CIASE), which allows a PLC module to be automatically designated as a repeater in the cluster and prevents the others from repeating.

Each PLC module has four different repeater states:

- always repeater (fixed mode, repeater state)
- never repeater (fixed mode, no\_repeater state)
- auto-active repeater mode, (dynamic mode, repeater state)
- auto-active non repeater mode (dynamic mode, no\_repeater state)

This function is activated at regular intervals. It sends a frame with a specific structure which, for each module configured in "auto mode", triggers an algorithm allowing it to choose whether or not it should repeat.

The repeater clusters are managed entirely automatically and no operator intervention is required.

Modules that are not in one of the "Auto mode" states disregard the repeater state automatic management frames sent by the concentrator.

The repeater call function is explained in detail in the chapter describing the repeater call function on the physical layer.

## 5. PLC COMMUNICATION SECURITY

This chapter only applies to Linky meters.

The security of the communications between the concentrator and the meters can be ensured by the services provided by the COSEM application protocol [13].

Each meter must have a CCC secret key, a unique CC\_LAN key, a unique CC\_LOCALE key and two session keys for the LAN interface (Read/Write and Broadcast sessions) and a session key for the Local interface transmitted when the application association with the Client concerned was created (see section 2.1.2 Reference model for the Linky meter).

The LAN (PLC) and LOCAL (EURIDIS Remote reporting) communication interfaces use the same security principles. The LOCAL interface can be activated or deactivated by a configurable object that specifies, when activated, whether this interface must be made secure. For this reason, the unique CC\_LAN and CC\_LOCALE keys, the session keys and the initialisation vectors are independent of the two interfaces. On the other hand, the CCC key is common.

### 5.1 Encryption method

128-bit AES symmetrical key algorithm, GCM operation mode. It is used to ensure data confidentiality and authentication.

The security tools are implemented on the application layer. Encryption and authentication also apply to the application data units (see [14] Cosem Green Book DLMS UA 1000-2:2008 7th edition).

#### 5.1.1 Initialisation vector

The initialisation vector is coded on 12 bytes containing a fixed part that identifies the data generating device and a random part.

The following principle will be used:

The order will be MSB to LSB.

- Six bytes corresponding to the ADS identifying the concentrator or the meter (see section 4.2 Equipment identification ).
- Two zero bytes.
- Four bytes corresponding to the value of a sent frame counter.
  - For a concentrator or TSP: counts all the requests sent to the modules
  - For a meter: counts the responses sent by the module to the concentrator or TSP.

### 5.2 "CCC" secret key

The CCC key is used to reprogram the "CC\_LAN" key or the "CC\_LOCALE" key in a meter.

This key is never used to encrypt the communications between the concentrator and the meter. It is known only to the meter and the IS. When the CC\_LAN (and the CC\_LOCALE respectively) is generated, the IS encrypts it with the CCC and transfers it to the counter via the concentrator. This transfer is completely transparent for the concentrator which sends the crypted data to the meter. The meter that knows the CCC is responsible for decryption the data in order to retrieve the CC\_LAN (and the CC\_LOCALE respectively).

The CCC key is not accessible in read mode.

### **5.3 Unique "CC\_LAN" and "CC\_LOCALE" keys**

The CC\_LAN and CC\_LOCALE keys are only used during the application association phase between the concentrator (Client application process) and the meter (Server application process) and the TSP and the meter respectively.

They are used to crypt the service allowing this application association. This service transfers the session key that will then be used, in the context defined by this application association, to crypt the communications between the concentrator/TSP and the meter.

In the case of an application association corresponding to a crypted application context, the session key is mandatory.

The CC\_LAN and CC\_LOCALE keys cannot be accessed in read mode.

### **5.4 Session keys**

The application association between the Public Client and the "Linky Meter" Logical Device is created in non crypted mode. The corresponding application context does not require a session key.

#### **5.4.1 LAN interface**

The application association between the Client R/W and the "Linky Meter" Logical Device is created in crypted mode. The corresponding application context requires a session key.

The application association between the Broadcast Client and the "Linky Meter" Logical Device is created in crypted mode. The corresponding application context requires a session key.

#### **5.4.2 LOCAL interface with encryption**

The application association between the Client R/W and the "Linky Meter" Logical Device is created in crypted mode. The corresponding application context requires a session key.

#### **5.4.3 LOCAL interface without encryption**

The application association between the Client R/W and the "Linky Meter" Logical Device is created in non crypted mode. The corresponding application context does not require a session key.