



**OPEN meter**

Open Public Extended Network metering



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Partners:** Iberdrola, Itron, ADD, ERSE, CTI, DLMS UA, EDF, Endesa, Enel, Kema, L+G, RWE, STMicroelectronics, University Karlsruhe, uSysCom, ZIV Medida

**Responsible:** Iberdrola

**Circulation:**  **Public**  
 **Confidential**  
 **Restricted**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**1/83

## D 3.1

# DESIGN OF THE OVERALL SYSTEM ARCHITECTURE

**DUE DELIVERY DATE:** 31-12-2009

**ACTUAL DELIVERY DATE:** 08-02-2010

© Copyright 2010 The OPEN meter Consortium



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**2/83

## Document History

Vers.	Issue Date	Content and changes
0.1	28.05.09	ToC proposal
0.2	30.11.09	Contributions on Protocol Architecture added
0.3	07.12.09	Draft on most sections and Protocol Architecture detailed
0.4	24.12.09	All profiles agreed, second round of comments included
1.0	21.01.10	Final comments, figures updated
1.1	08.02.10	Update with Technical Board comments

## Document Authors

Partners	Contributors
Itron	Auguste Ankou, Gloria Romero
ADD	Andres Muñoz
ERSE	Giuseppe Mauri, Diana Moneta
CTI	Weilin Liu, Jacek Wikiera
DLMS UA	Gyozo Kmethy
EDF	Gaizka Alberdi, Aline Pajot
Endesa	Amador Gomez, Carmelo Rodriguez
Enel	Giuseppe Fantini
Iberdrola	Inigo Berganza
Kema	Dieter Gutschow
L+G	Christoph Rahm
STMicroelectronics	Nunzio DiPaola, Alessandro Lasciandare, Alessandro Moscatelli
University Karlsruhe	Michael Bauer, Martin Sigle
uSysCom	Aitor Arzuaga, Laura Marron
ZIV Medida	Exabier Bilbao



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**3/83

## Document Approvers

Partners	Approvers
CTI	Markus Bittner
Endesa	Robert Denda
Iberdrola	Iñigo Berganza
Kema	Willem Strabbing
L+G	Thomas Schaub



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**4/83

**TABLE OF CONTENTS**

<b>1</b>	<b>EXECUTIVE SUMMARY</b> .....	<b>9</b>
<b>2</b>	<b>INTRODUCTION</b> .....	<b>10</b>
2.1	OBJECTIVE AND SCOPE .....	10
2.2	STRUCTURE OF THE DOCUMENT .....	13
2.3	NOTATIONS, ABBREVIATIONS AND ACRONYMS .....	14
2.4	REFERENCES.....	18
	<b>PART I – OPEN METER SYSTEM GLOBAL ARCHITECTURE AND COMPONENTS</b> .....	<b>20</b>
<b>3</b>	<b>SYSTEM ARCHITECTURE OVERVIEW</b> .....	<b>20</b>
3.1	INTRODUCTION AND RATIONALE.....	20
3.2	SYSTEM MODULES AND INTERFACES.....	20
<b>4</b>	<b>MODULES</b> .....	<b>24</b>
4.1	INTRODUCTION.....	24
4.2	ELECTRICITY METER/COMMUNICATION HUB .....	25
4.3	CONCENTRATOR .....	26
4.4	CENTRAL SYSTEM.....	27
4.5	LEGACY SYSTEMS .....	28
4.6	LOCAL O&M DEVICES .....	28
4.7	MULTI-UTILITY METER.....	29
4.8	END CUSTOMER DEVICES.....	29
4.9	EXTERNAL DEVICES.....	29
<b>5</b>	<b>INTERFACES</b> .....	<b>30</b>
5.1	MI1-CI1.....	30
5.2	MI2-SI2.....	30
5.3	MI3.....	30
5.4	MUMI2.....	31
5.5	MUMI1-MI4 .....	31
5.6	MI5.....	31
5.7	CI2-SI1 .....	32
5.8	CI3 .....	32
5.9	CI4.....	32
	<b>PART II – COMMUNICATION PROFILES FOR OPEN METER SYSTEM INTERFACES</b> .....	<b>33</b>
<b>6</b>	<b>SECURITY</b> .....	<b>33</b>
6.1	SECURITY NEEDS .....	33
6.2	SECURITY FEATURES OF DLMS/COSEM .....	34
6.2.1	<i>Introduction</i> .....	34
6.2.2	<i>Data access security</i> .....	34
6.2.3	<i>Data transport security</i> .....	36
6.3	SECURITY IN LOWER LAYERS.....	40
<b>7</b>	<b>MI1-CI1 (ELECTRICITY METER/COMMUNICATION HUB-CONCENTRATOR)</b> .....	<b>41</b>
7.1	INTRODUCTION.....	41
7.2	ARCHITECTURE OF THE DLMS/COSEM S-FSK PLC PROFILE .....	43
7.2.1	<i>Physical layer</i> .....	43



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**5/83

7.2.2	Data Link layer.....	44
7.2.3	Networking Layers (Network, Transport).....	45
7.2.4	Upper layers (Session, Presentation, Application).....	45
7.2.5	Data Model.....	45
7.2.6	Security.....	47
7.3	ARCHITECTURE OF THE DLMS/COSEM PRIME PLC PROFILE.....	48
7.3.1	Physical Layer.....	49
7.3.2	Data Link Layer.....	50
7.3.3	Convergence layers.....	52
7.3.4	Networking Layers (Network, Transport).....	55
7.3.5	Upper layers (Session, Presentation, Application).....	55
7.3.6	Data Model.....	55
7.3.7	Security.....	55
<b>8</b>	<b>MI2-SI2 (ELECTRICITY METER/COMMUNICATION HUB-CENTRAL SYSTEM).....</b>	<b>57</b>
8.1	INTRODUCTION.....	57
8.2	SUBNETWORK LAYERS.....	58
8.2.1	GPRS (2.5G).....	59
8.2.2	UMTS (3G).....	59
8.3	NETWORKING LAYERS.....	60
8.3.1	Network layer: IPv4/IPv6.....	60
8.3.2	Transport layer.....	61
8.4	APPLICATION LAYERS.....	61
8.5	DATA MODEL.....	61
8.6	SECURITY.....	61
<b>9</b>	<b>MI3 (ELECTRICITY METER/COMMUNICATION HUB-LOCAL O&amp;M DEVICE).....</b>	<b>62</b>
9.1	INTRODUCTION.....	62
9.2	DLMS/COSEM OVER OPTICAL INTERFACE.....	62
9.2.1	Physical Layer.....	63
9.2.2	Data Link Layer.....	63
9.2.3	Application Layer.....	64
9.2.4	Data Model.....	64
<b>10</b>	<b>MUMI2 (MULTI-UTILITY METER-LOCAL O&amp;M DEVICE).....</b>	<b>65</b>
10.1	INTRODUCTION.....	65
<b>11</b>	<b>MUMI1-MI4 (MULTI-UTILITY METER - ELECTRICITY METER/COMMUNICATION HUB).....</b>	<b>66</b>
11.1	INTRODUCTION.....	66
11.2	M-BUS TWISTED PAIR.....	67
11.2.1	Physical layer.....	68
11.2.2	Data link layer.....	68
11.2.3	Network/transport layer.....	68
11.2.4	Application layer.....	68
11.3	M-BUS TWISTED PAIR DLMS/COSEM.....	68
11.3.1	Physical layer.....	68
11.3.2	Data link layer.....	69
11.3.3	Application layer.....	69
11.4	WIRELESS M-BUS.....	69
11.4.1	Introduction.....	69
11.4.2	Physical layer.....	69



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**6/83

11.4.3	Data link layer .....	70
11.4.1	Network/transport layer .....	70
11.4.2	Application layer .....	70
11.5	EURIDIS2 DLMS/COSEM .....	70
11.5.1	Physical layer.....	71
11.5.2	Data link layer .....	71
11.5.3	Transport layer .....	71
11.5.4	Support manager layer.....	71
11.5.5	Application layer .....	71
11.6	IEEE 802.15.4 RADIO.....	71
11.7	ZIGBEE .....	71
11.7.1	Physical layer.....	72
11.7.2	Data link layer .....	72
11.7.3	Network/transport layer .....	72
11.7.4	Application layer .....	72
<b>12</b>	<b>MI5 (ELECTRICITY METER/COMMUNICATION HUB-END CUSTOMER DEVICES) .....</b>	<b>73</b>
12.1	INTRODUCTION.....	73
12.2	COMMUNICATION PROFILES PROPOSAL .....	73
<b>13</b>	<b>CI2-SI1 (CONCENTRATOR-CENTRAL SYSTEM) .....</b>	<b>75</b>
13.1	INTRODUCTION.....	75
13.2	PHYSICAL LAYERS .....	75
13.3	NETWORK AND TRANSPORT LAYERS.....	75
13.4	PROTOCOL PROFILES .....	75
13.4.1	Profile 1 - SNMPv3 and sftp.....	76
13.4.2	Profile 2: Web Services-based profile .....	77
<b>14</b>	<b>CI3 (CONCENTRATOR-LOCAL O&amp;M DEVICE) .....</b>	<b>79</b>
14.1	INTRODUCTION.....	79
<b>15</b>	<b>CI4 (CONCENTRATOR-EXTERNAL DEVICES) .....</b>	<b>80</b>
15.1	INTRODUCTION.....	80
15.2	PROTOCOL ASSESSMENT .....	80
15.2.1	Possible solutions .....	80
15.2.2	Status of protocols.....	82
<b>16</b>	<b>COPYRIGHT.....</b>	<b>83</b>



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**7/83

**List of Figures**

Figure 1 - OPEN meter System Architecture.....	21
Figure 2 - OPEN meter architecture compared to M/441 .....	23
Figure 3 – LLS and HLS authentication .....	36
Figure 4 – Data transport security in DLMS/COSEM.....	37
Figure 5 – Ciphered xDLMS APDUs.....	39
Figure 6 - MI1-CI1 architecture .....	42
Figure 7 - DLMS/COSEM S-FSK PLC architecture.....	43
Figure 8 - COSEM application model of a Concentrator and metering equipment.....	46
Figure 9 - DLMS/COSEM PRIME PLC architecture .....	48
Figure 10 - MI2–SI2 interface communications architecture.....	58
Figure 11 - Protocol overview of the GPRS network. ....	59
Figure 12 - UTRAN protocol layering, interfaces and specification references .....	60
Figure 13 - MI3 interface communications architecture .....	63
Figure 14 - MUMI1-MI4 interface profiles.....	67
Figure 15 - ZigBee stack architecture .....	72
Figure 16 - MI5 interface profiles .....	74
Figure 17 - The two profiles for CI2-SI1 .....	76
Figure 18 - IEC 61850 stack and messages .....	81
Figure 19 - IEC 61850 family and link with other standards .....	82



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**8/83

**List of Tables**

Table 1 - Overview of system functions..... 10  
Table 2 - Overview of technologies and protocols selected in [3] ..... 21  
Table 3 – System interfaces and related components..... 22  
Table 4 – Overview of Security requirements..... 33  
Table 5 – Security suites..... 38  
Table 6 – Security control byte..... 40  
Table 7 - MUMI1-MI4 interface communication architecture choices ..... 66  
Table 8 - complete IEC 61850 stack and links with other standards..... 81



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**9/83

## 1 Executive summary

D3.1 is the main outcome of OPEN meter Task 3.1 “Initial definition of the architectural model based on OSI conceptualization”.

The purpose of this document is to provide a complete Architecture for the OPEN meter AMI. Previous work considered includes [1], [2] and [3].

Note that technologies assessed and selected in [2], along with gaps analyzed in [3], were taken as an important input, but not necessarily exclusive. Further selection of technologies and protocols is performed in this document.

More than one profile is sometimes defined per communications interface. All of them are considered to comply with OPEN meter requirements, and thus have been kept in the Architecture.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**10/83

## 2 Introduction

### 2.1 Objective and Scope

The present document “Design of the overall System Architecture” represents the first deliverable coming out of the work of WP3 “Pre-normative research activities” within the OPEN meter Project. This document takes as inputs the definition of the OPEN meter system components and interfaces presented in WP1, and the selection of technologies carried out within WP2.

For the elaboration of this document every input has been analyzed from a technical point of view, in order to provide a sound technical framework for the following activities within the project.

It also has to be mentioned that even though every interface presented in the System Architecture will be analyzed, interfaces CI4 and MI5 will not be further analyzed. This is because requirements for End Customer devices and External devices have not been specified (see Figure 1).

The objective of this document is to select specific technology solutions for the Protocol Architecture of each of the interfaces. Each interface will be analyzed following the OSI layer model, and thus each layer will be assigned a certain protocol in order to provide full communication stacks for each interface. These communications stacks are usually called Functional Profiles (the “function” being here the service of the interface), Communication Profiles or just “profiles”. Also the interfaces between layers and the functionality of each of these layers and interfaces will be discussed.

The OPEN meter Project has adopted this approach to be able to incorporate new technologies in a later stage. The architectural model gives the conditions for new technologies to be included: they should match with the other elements chosen for the profiles.

The resulting Protocol Architectures will be further analyzed in subsequent WP3 Tasks, where the resulting technology gaps will be studied and solutions proposed in order to provide a complete end-to-end communication system structure for AMI.

Table 1, based on [1] gives an overview of the OPEN meter System Requirements OM-SR1 to OM-SR20. Each and every System Requirement can be mapped on a one-to-one basis to a single Use Case, which is also described in the table.

The Use Cases have also been mapped to the “High level additional functionalities” specified by the European Smart Metering Standardization Mandate M/441 Smart Metering Coordination Group in [4]. The mapping is not complete in either direction.

Table 1 - Overview of system functions

Function category	Use case ID	Use Case	Description	M/441 functionality (see [4])
Minimum	OM-SR1	Meter Registration	Process of incorporating meters to the remote managed equipment grid	F.2.(b)
Minimum	OM-SR2	Remote Tariff Programming	Process of remotely programming in the meter those parameters related to tariff,	F.2 (b)



**Work Package:** WP3

**Type of document:** Deliverable

**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 Page:11/83

Function category	Use case ID	Use Case	Description	M/441 functionality (see [4])
			calendars and contracted power	
Minimum	OM-SR3	Meter reading (On demand)	Process of gathering and providing on demand meter readings in answer to a specific request	F.1
Minimum	OM-SR4	Meter reading (for billing)	Process of gathering and providing meter readings for billing process (cycle reading)	F.1
Minimum	OM-SR5	Remote Disconnection and Reconnection	Process of remotely disconnect or reconnect the supply of electrical power to a customer on a designated date	F.4 (a)
Minimum	OM-SR6	Power control	Process of activating or deactivating the demanded power control mode in meters	F.4 (b)
Minimum	OM-SR7	Clock Synchronization	Process of adjusting the internal clock of metering equipments	F.2 (b)
Minimum	OM-SR8	Remote Firmware Update	Process of remote update of meters firmware	F.2 (b)
Minimum	OM-SR9	Alarm and event Management	Process of management of events and equipment alarms	F.2 (a)
Minimum	OM-SR10	Interruption information	Process of obtaining interruption information	F.2 (a)
Minimum	OM-SR11	Fraud Detection	Process to detect any possible fraud cases	F.2 (a)
Minimum	OM-SR12	Remote Concentrator access (Registration /Programming /Reading /Firmware Update)	Process of remote management of Concentrators	-
Minimum	OM-SR13	Load Profile Management	Process of remote programming and gathering of load profile	F.1 (a)
Advanced	OM-SR14	Automatic adaptation to grid changes	Process of automatic adaptation of grid topology changes	-
Advanced	OM-SR15	Meter Availability Control	Process of checking the communication with meters	-
Optional	OM-SR16	Energy Balances	Process of obtaining energy balances	-
Optional	OM-SR17	Load Management	Process of activating or deactivating the demanded power control mode in meters in certain situations	F.4 (b)
Optional	OM-SR18	Customer device management	Process of sending measures related to customer supply energy	F.2
Optional	OM-SR19	Power Quality Management	Process of gathering power quality measurements	F.2.(a)
Optional	OM-SR20	Prepayment	Process of managing prepayment functionality for the energy consumption of the	F.3 (a)



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**12/83

Function category	Use case ID	Use Case	Description	M/441 functionality (see [4])
			customer	



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**13/83

## 2.2 Structure of the document

This Chapter 2 provides an introduction, outlines the purpose and provides useful information for understanding D3.1. The document is further divided into two Parts.

“PART I – OPEN meter System global Architecture and components” includes Chapters 3 to 5. In these we will deal with the System Architecture, explaining it and detailing its two main elements: interfaces and modules.

“PART II – Communication Profiles for Open Meter System Interfaces” includes chapters 6 to 15, where the Protocol Architecture for each and every of the OPEN meter interfaces is described. As explained above, for a certain interface the selected complete communication profiles will be given.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**14/83

## 2.3 Notations, abbreviations and acronyms

AA	Application Association
ACSE	Association Control Service Element
AE	Application Entity
AES	Advanced Encryption System
AMI	Advanced Metering Infrastructure
AP	Application Process
APDU	Application-layer PDU
ARQ	Automatic Repeat Request
ASE	Application Service Element
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization (also CLC)
Cix	Concentrator Interface x
CIASE	Configuration Initiation ASE
COSEM	Companion Specification for Energy Metering
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTT	Conformance Test Tool (DLMS/COSEM)
DHCP	Dynamic Host Control Protocol
DLC	Distribution Line Carrier (same concept as PLC)
DLMS	Distribution Line Message Specification (IEC 61334-4-41) or Device Language Message Specification (IEC 62056)
DSO	Distribution System Operator
Dx.y	OPEN meter Deliverable y in WPx
EN	European Norm



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**15/83

ETSI	European Telecommunications Standards Institute
EU	European Union
EUI-48	Extended Unique Identifier – 48 bit (MAC Address)
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
HA	Home Automation
HAN	Home Area Network
HDLC	High-Level Data Link Control
IANA	Internet Assigned Numbers Authority
IC	Interface class (COSEM)
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
LD	Logical Device (COSEM)
LLC	Logical Link Control
LSDU	LLC-layer SDU
LV	Low Voltage
M-Bus	Meter-Bus
M/441	Standardization Mandate 441
MAC	Medium Access Control
Mlx	Meter Interface x
MIB	Management Information Base
MUMlx	Multi-utility meter Interface x



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**16/83

MV	Medium Voltage
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OBIS	Object Identification System
OPEN meter	Open Public Extended Network metering
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PHY	Physical layer
PLC	Power Line Communications
PRIME	Powerline Intelligent Metering Evolution
PSTN	Public Switched Telephone Network
RFC	Request for Comments (IETF memorandum)
RNC	Radio Network Controller
S-FSK	Spread Frequency Shift Keying
SAP	Service Access Point
SCADA	Supervisory Control And Data Acquisition
SDU	Service Data Unit
SEP	Smart Energy Profile (ZigBee)
Slx	Central System Interface x
SML	Smart Message Language
TC	Technical Committee
TCP	Transmission Control Protocol
TP	Twisted Pair



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**17/83

UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network
WPx	OPEN meter Working Package x
xDLMS	Extended DLMS
xDSL	x (generic) Digital Subscriber Line



Work Package: WP3

Type of document: Deliverable

Date: 08/02/2010

Energy Theme; Grant Agreement No 226369

Title: Design of the overall System Architecture

Version: 1.1 Page:18/83

## 2.4 References

#	Ref.	Title
[1]	OPEN meter D1.1	<i>REPORT ON THE IDENTIFICATION AND SPECIFICATION OF FUNCTIONAL, TECHNICAL, ECONOMICAL AND GENERAL REQUIREMENTS OF ADVANCED MULTI-METERING INFRASTRUCTURE, INCLUDING SECURITY REQUIREMENTS</i>
[2]	OPEN meter D2.2	<i>ASSESSMENT OF POTENTIALLY ADEQUATE TELECOMMUNICATIONS TECHNOLOGIES - GENERAL REQUIREMENTS AND ASSESSMENT OF TECHNOLOGIES</i>
[3]	OPEN meter D2.3	<i>IDENTIFICATION OF RESEARCH NEEDS FROM BOTTOM-UP APPROACH KNOWLEDGE GAPS</i>
[4]	SMART METERS CO-ORDINATION GROUP FINAL REPORT (Version 0.7 – 2009-12-10)	<i>Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability - M/441</i>
[5]	DLMS UA 1000-2 Ed. 7.0:2009	<i>DLMS/COSEM Architectures and Protocols, "Green Book"</i>
[6]	FIPS PUB 197:2001,	<i>Advanced Encryption Standard (AES)</i>
[7]	IEC 61334-5-1 Ed. 2.0:2001	<i>Distribution automation using distribution line carrier systems – Part 5-1: Lower layer profiles – The spread frequency shift keying (S-FSK) profile</i>
[8]	PRIME v1.3a	<i>PRIME: Draft Standard for Powerline Intelligent Metering Evolution (available at <a href="http://www.prime-alliance.org">http://www.prime-alliance.org</a>)</i>
[9]	IEC 61334-4-32 Ed. 1.0:1996	<i>Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 32: Data link layer – Logical link control (LLC)</i>
[10]	ISO/IEC 8802-2 Ed. 3.0:1998	<i>Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control</i>
[11]	IEC 62056-53 Ed 2.0:2006	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 53: COSEM Application layer</i>
[12]	ISO/IEC 8649 Ed. 2.0:1996	<i>Information technology – Open Systems Interconnection – Service definition for the Association Control Service Element</i>
[13]	ISO/IEC 8650-1 Ed 2.0:1996	<i>Information technology – Open systems interconnection – Connection-oriented protocol for the association control service element: Protocol specification</i>
[14]	IEC 61334-4-41 Ed.1.0:1996	<i>Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocol – Distribution line message specification</i>
[15]	IEC 62056-62 Ed 2.0:2006	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 62: Interface classes</i>
[16]	IEC 62056-61 Ed 2.0:2006	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 61: OBIS Object identification system</i>
[17]	DLMS UA 1000-1 Ed. 9.0:2009	<i>COSEM Interface Classes and the OBIS Identification System, "Blue Book"</i>
[18]	EN 50065-1:2001	<i>Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148,5 kHz - Part 1: General requirements, frequency bands and electromagnetic disturbances</i>
[19]	IEC 61334-4-1	<i>Distribution automation using distribution line carrier systems – Part 4:</i>



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**19/83

Ed. 1.0:1996	<i>Data communication protocols – Section 1: Reference model of the communication system</i>
[20] STD0005 (1981)	<i>Internet Protocol (Also: RFC0791, RFC0792, RFC0919, RFC0922, RFC0950, RFC1112)</i>
[21] IEC 62056-47 Ed 1.0:2006	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 47: COSEM transport layer for IP networks</i>
[22] STD0006 (1980)	<i>User Datagram Protocol (Also: RFC0768)</i>
[23] OPEN meter D2.1	<i>DESCRIPTION OF CURRENT STATE-OF-THE-ART OF TECHNOLOGY AND PROTOCOLS</i>
[24] NIST SP 800-57:2007	<i>Recommendation for Key Management – Part 1: General (Revised)</i>
[25] RFC2460	<i>Internet Protocol, Version 6 (IPv6) Specification</i>
[26] RFC3316	<i>Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts</i>
[27] IEC 62056-21 Ed 1.0:2002	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange</i>
[28] IEC 62056-42 Ed.1.0:2002	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange</i>
[29] IEC 62056-46 Ed.1.1:2007	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol</i>
[30] EN 13757-2:2004	<i>Communication systems for remote reading of meters. Physical and link layer</i>
[31] EN 13757-3:2004	<i>Communications systems for and remote reading of meters. Dedicated application layer</i>
[32] EN 13757-4:2005	<i>Communication systems for meters and remote reading of meters. Wireless meter readout (radio meter reading for operation in the 868-870 MHz SRD band)</i>
[33] EN 13757-1:2002	<i>Communication system for meters and remote reading of meters. Data exchange</i>
[34] ISO/IEC 13239 Ed. 3.0:2002	<i>Information Technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures</i>
[35] IEC 62056-31 Ed 2.0:200x	<i>Electricity metering – Data exchange for meter reading, tariff and load control – Part 31: Use of local area networks on twisted pair with carrier signalling</i>
[36] STD0007 (1981)	<i>Transmission Control Protocol. Also: RFC0793</i>



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**20/83

# **PART I – OPEN meter System global Architecture and components**

## **3 System Architecture Overview**

### **3.1 Introduction and rationale**

PART I of this document focuses on the general System Architecture, which identifies modules (components) and interfaces connecting such components. Once the interfaces are defined, PART II will analyze the different Protocol Architectures for each and every interface.

The OPEN meter Project has defined (see [1]) a first reference architecture for a standardized European smart metering solution, based on the know-how of a representative set of large distribution utilities and major European equipment manufacturers.

This architecture is used as a reference framework to identify and specify functional, technical, economical and general requirements of an advanced multi-metering infrastructure, including security requirements, which serve as a guideline for the rest of the OPEN meter Project activities.

The definition of the requirements takes into account the needs of the different stakeholders and allows the OPEN meter technology to be modular and scalable to offer the correct and most cost-effective choice for all scenarios.

The proposed architecture takes into account the need for future evolutions and control of the distribution grid, by incorporating a device to be installed at the transformer stations, the Concentrator, which communicates with the Central System and manages the meters and devices installed at the customer premises. This naturally fits the structure of the electricity grid and allows electricity utilities to take advantage of assets owned by them (e.g. power line communications to remotely access meters over an existing, operated infrastructure).

For the case of multi-utility metering, a device called communication hub, which might either be integrated into a meter or operate as a separate device, has been added.

The proposed architecture is valid for a whole range of scenarios: small or large utilities, traditional or highly innovative companies. The OPEN meter architecture may be customized considering national regulations.

The architecture of the OPEN meter solution allows integrating various existing open technologies, achieving interoperability and coexistence of a collection of solutions that will consist of various communication protocols and physical modulations and allows for optional interfaces at the system component level.

### **3.2 System modules and interfaces**

Figure 1 below illustrates the different system components and interfaces that define the System Architecture for the OPEN meter Project.



**Energy Theme; Grant Agreement No 226369**

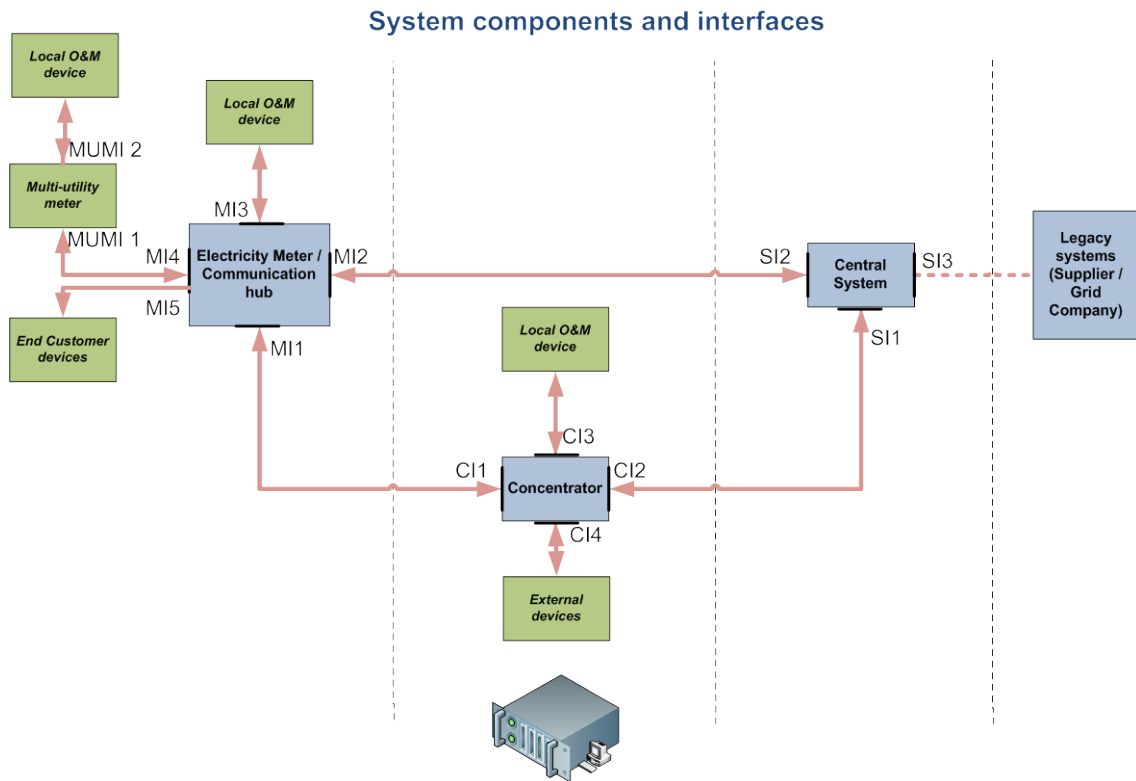


Figure 1 - OPEN meter System Architecture

[3] proposed the communication technologies, protocols and data models shown in Table 2 below.

Table 2 - Overview of technologies and protocols selected in [3]

Interface	Selected Technology Type	Selected Technologies and lower layer protocols	Selected Upper layer protocols	Selected Data Models
MI1–CI1	PLC	PRIME IEC 61334-5-1	DLMS SML	COSEM
CI2–SI1	Wireless	UMTS GPRS	DLMS SML	COSEM
MI2–SI2	Wireless	UMTS GPRS	DLMS SML	COSEM
MI3, CI3 and MUMI2	Wireless	IEEE802.15.4 IEEE802.11-2007	DLMS SML	COSEM
MUMI1-MI4	Wireless	IEEE802.15.4 IEEE802.11-2007 Wireless M-Bus	DLMS SML Wireless M-Bus	COSEM
CI4	Wireless	ZigBee WiFi	DLMS SML IEC 61850	COSEM
MI5	Wireless	Bluetooth	DLMS	COSEM



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**22/83

Interface	Selected Technology Type	Selected Technologies and lower layer protocols	Selected Upper layer protocols	Selected Data Models
		(IEEE802.15.1-2002) ZigBee	SML ZigBee SEP	

Note1: The SI3 interface is outside the Scope of the Project.  
 Note 2: For the MI2–SI2 interface, any technology capable to carry internet traffic (TCP/IP) should be suitable: for example optical cable, xDSL. There is no reason to limit to GPRS / UMTS.  
 Note 3: Wireless M-Bus has not been initially selected in the MUMI1-MI4 interface assessment. However this result is conditioned to IEEE802.11 being able to provide enough battery lifetime for multi-utility meters. If this were not the case for the next revision of Deliverable 2.2 (due 2010), then Wireless M-Bus would probably become a selected technology for this interface.

SML as an upper layer protocol has not been considered inside this version of the document (the reason being that SML is not considered sufficiently documented and fully standardized).

The interfaces between the system components can be summarized in Table 3. WP3 will focus on the interfaces that are highlighted in bold, as these are currently considered to be the main focus areas for the OPEN meter Project.

Table 3 – System interfaces and related components

System interface	System components	Local / Wide-Area communications
<b>CI2-SI1</b>	Concentrator - Central System	Wide-area
<b>MI2-SI2</b>	E-meter / Comms Hub - Central System	Wide-area
SI3	Central System - <i>Legacy systems (Supplier / Grid Company)</i>	N/A
<b>MI1-CI1</b>	E-Meter / Comms Hub - Concentrator	Local
CI3	Concentrator - Local O&M device	Local
CI4	Concentrator - <i>External devices</i>	Local
MI3	E-meter / Comms Hub - Local O&M device	Local
<b>MUMI1-MI4</b>	Multi-utility meter - E-meter / Comms Hub	Local
MI5	E-meter / Comms Hub - <i>End Customer devices</i>	Local
MUMI2	Multi-utility meter - Local O&M device	Local

Figure 2 attempts to consolidate the OPEN meter System Architecture specified in [1] with the identification of communication entities, interfaces and standardization responsibilities as specified by the Smart Metering Coordination Group developing the coordinated response of the European Standardization Organizations to the Smart metering Standardization Mandate M/441 of the European Commission (see [4]).



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**23/83

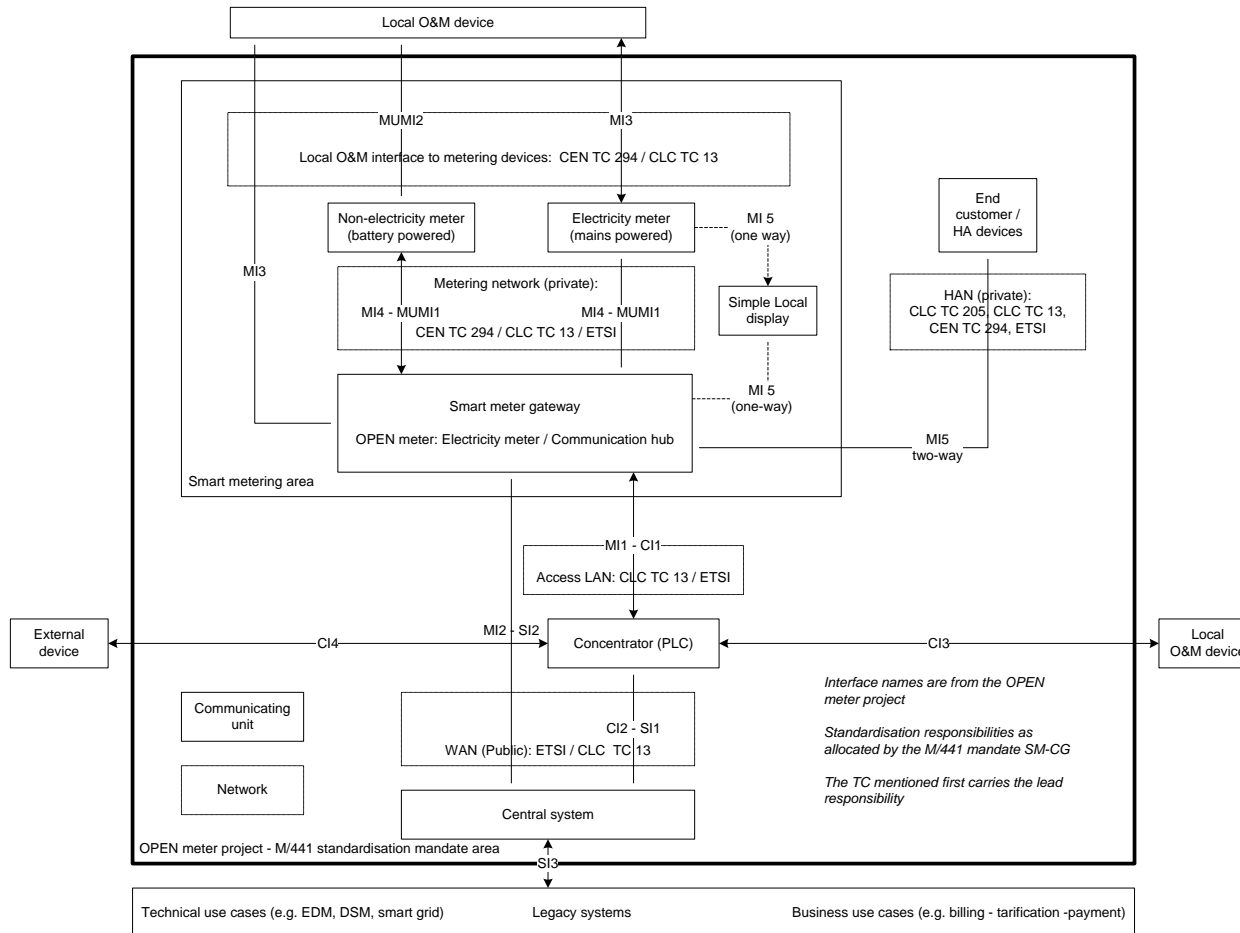


Figure 2 - OPEN meter architecture compared to M/441



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**24/83

## 4 Modules

### 4.1 Introduction

The objective of the OPEN meter project is to specify solutions for a multi-utility smart metering system, covering electricity, gas, water and heat alike.

Between the meters of these kinds of energies, some important differences exist:

- The electricity meter is the only one permanently powered, whereas the meters for other kinds of energy are generally battery powered, and battery lifetime is of key economic and operational importance;
- It is expected, that the penetration of smart metering will be the largest in electricity metering. This statement is substantiated by the following:
  - According to EU Directive 2009/72, concerning common rules for the internal market in electricity, where roll-out of smart meters is assessed positively, at least 80% of consumers shall be equipped with intelligent metering systems by 2020;
  - According to EU Directive 2009/73, concerning common rules for the internal market in natural gas, no target dates and figures are specified, only the preparation of a timetable for the implementation of intelligent metering systems. The reason for this important difference is that when gas is not used for heating, and as load management and tariffication today is less interesting in gas metering than in electricity metering, it is more difficult to build a positive business case.
  - No similar Directives establishing target figures for smart metering exist for heat and water meters. Often there are several units installed per house/flat.
- Electricity meters are directly connected to the electricity network, which may be conveniently used as a media for data exchange. Connection of other meters to the electricity network would bring up safety and cost issues.

Therefore, the electricity meter can be used advantageously as the communication hub for the other multi-utility meters.

However, the OPEN meter Project covers various scenarios, depending on market organization, economical and technical conditions. Some of the possible scenarios are listed below:

- The only smart meter in the house is the electricity meter. In this case the Electricity meter acts as communication hub. If the owner of the network is not the owner of the meter the communication part may be separated from the meter;
- There are several smart meters for various kinds of supply in the house, and their owners – typically the Distribution System Operators – agree on using of a common smart metering infrastructure. In this case, the Electricity Meter/Communication hub may be the electricity meter or it may be a separate device, to which all meters are connected;



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**25/83

- There are several smart meters for various kinds of supply, but the DSOs do not share a common infrastructure. In this case, each meter may serve as a communication hub to other multi-utility meters, exchanging data with the Central System, directly or via the Concentrator.

## 4.2 Electricity Meter/Communication hub

The Electricity Meter/Communication hub is an electronic smart device which has two basic functionalities. First, it measures and records electrical energy consumed or produced as well as other electrical quantities, and secondly it acts as a communication hub regarding several devices. It is capable of functioning as a communication hub, because it is connected to mains power, in contrast with other metering devices which are usually battery-powered. In some cases the communication hub can be a dedicated device which provides Gateway or Proxy functionalities exclusively, without electricity meter capabilities.

As a communication hub, the electricity meter incorporates additional processing capabilities, memory and communications means for storage and transmission of data. Its main purpose is to facilitate correct and efficient data transfer / communication between the in-home network devices and the external AMI network. The in-home network devices could represent multi-utility meters (water, gas, heat, and the electricity meter itself) accessed via MI4, as well as other user interface devices accessed via MI5 (e.g. a Home Display Unit).

The Electricity Meter/Communication hub may operate in two different modes:

- It may operate as a Proxy Gateway; or
- It may operate as a Gateway.

In the first case, it collects and stores data from the other meters, and the central system normally accesses these stored data. However, direct access should be also possible, for example to support on-demand reading or e.g. to operate a gas valve.

In the second case it operates as a Gateway and the central system directly accesses the data in each meter directly.

Most multi-utility meters exhibit inherent constraints, which are mainly owed to the fact that they are battery-operated with long battery-lifetime expectancy. Since this energy constraints do not allow the devices to be “always on” or “always receive”, the associated interface (MUMI1-MI4) is not fully bi-directional, in the sense that a multi-utility device will only receive after itself initiated a send operation. Thus spontaneous interaction with the multi-utility meter will most likely not be possible, making the pure Gateway function unfeasible.

Moreover the periodic (and partly redundant) transmissions of the multi-utility meters might preferably be buffered in the Proxy Gateway instead of forwarding them straight away to higher levels. Spontaneous reads of the virtual multi-utility meter object in the Proxy Gateway are then possible.

The same buffering capability is needed for downstream commands to a multi-utility meter, where the Proxy Gateway will buffer the information until it can be delivered to the multi-utility meter.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**26/83

Depending on the Electricity Meter/Communication hub working mode, the multi-utility meters will communicate with the system through the Gateway or through demands to be managed by the Proxy Gateway.

Protocols used on the MI1-CI1 interface or MI2-SI2 interface may be different from those used on MUMI1-MI4 or MI5 interfaces. Therefore a protocol translation is needed inside the communication hub in case the of a Gateway approach. In the case of a Proxy Gateway, the Electricity Meter/Communication hub acts as a server at the MI1-CI1 or MI2-SI2 interface, and as client/master at MUMI1-MI4 interface. In the case of two-way communication on the MI5 interface, it also acts as a server towards the end Customer device.

Additionally the electricity meter also allows for local access by an operation and maintenance handheld-type device via the local interface MI3.

The Electricity Meter/Communication hub is remotely managed by the Central System, either directly through the wide-area communication interface MI2, if present, or indirectly via a Concentrator using interface MI1.

### 4.3 Concentrator

The Concentrator is an intermediate element between the Electricity Meter/Communication hub and the Central System. It is necessary when the local network uses power line communications as a media. It is typically located inside an electrical MV/LV substation.

Its main tasks are the following:

- To build up, maintain and manage the PLC network for communication with meters. The strategy to perform this activity may depend on the PLC technology used;
- To exchange data with the Electricity Meter/Communication hub (CI1 interface);
- To exchange data with the central system (CI2 interface);
- To optionally provide data to other systems (e.g. SCADA) via the CI4 interface.

The Concentrator is thus responsible for collecting and managing the information received from the electricity meters, directly, and indirectly from the multi-utility meters, if present, as well as, also indirectly, from the end-customer devices, if present. This information, consisting of measurement registers, alarms, etc. which is collected through CI1 is subsequently sent to the Central System.

For control commands, programming, reconfigurations, etc. coming from the Central System, the data flow is the opposite direction and it reaches the Electricity Meter/Communication hub via MI1.

Similarly to the Electricity Meter/Communication hub, it may act as a Proxy Gateway for the meters, collecting data from them, sending data and commands to them, and forwarding the stored data to the Central System. It should support direct access from the Central System to the meters, to support on-demand reading, or to send direct commands (e.g. enabling / disabling supply to the premises).



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**27/83

The Concentrator also has an interface CI3 for connecting a local operation and maintenance device. The option also exists to connect external devices via the CI4 interface.

## 4.4 Central System

The Central System is responsible for the management of all information and data related to Smart Metering. Ultimately it is also responsible for the configuration, control and operation of all system components using communications via the wide-area interfaces SI1 and SI2. Its functionality includes the treatment of events and alarms too, and the management and operation of all communication systems.

It interfaces with Legacy Systems through SI3. A Legacy System could be a Customer Commercial System that manages the customers' supply 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 Central System to send, for example, messages related to energy supplying contract or simply to advertise the customers.

The Central System:

- Receives (from Legacy Systems) work orders and commands to accomplish a request toward the network;
- Ensures their timely and correct execution;
- Sends back acknowledgments and operation's results.

Orders may include reading of measurement data and parameters, reconfiguration of field components, remote disconnect of supply, etc. The Central System might delegate parts of its operation to the Concentrators, if present, such that certain operations can be performed locally without the need of continuous wide-area communications.

When the Central System receives a request on SI3 interface, from any kind of Legacy System, it has to:

- Translate the customer's "legacy ID" in "network ID" using a sort of "routing table" managed in its database containing a repository of data and information about network architecture, and description of available nodes.
- Translate the Legacy request in a command's sequences of appropriate communication protocol, depending on characteristics of used interface and involved devices.
- Send results of previous steps towards the network, also using a communication management subsystem, if it is present.

In case of messages coming up from the network towards Legacy Systems, the Central Systems have to dispatch the arriving message to the respective Legacy System, depending on which kind of message has been received (for instance Energy Supplying Management messages as well as Billing Data, Network alarms or management reporting).



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**28/83

The Central System is the basic component within an AMI system; it performs the de-coupling between the utilities legacy Systems and their field's devices, making itself responsible for using right paths and adequate protocols to manage any kind of devices (meters and/or Concentrators) which could have features, behavior and functioning very different from one another.

## 4.5 Legacy Systems

The Legacy Systems refers to one or more existing commercial or technical systems within a DSO that is responsible for the management of business processes such as meter registration, remote meter reading, tariff adjustment, remote connect/disconnect, billing, outage management etc.

In terms of the OPEN meter architecture the Central System is responsible to communicate with the meters. This means that the Legacy Systems do not need to know anything about the meter communications infrastructure, communications protocols or technologies. It can therefore focus only on its core functions which are to support the operational and business processes. This also means that the Legacy Systems can effectively operate independently from any specific metering or communications technology.

The Legacy Systems interface with the Central System via interface SI3. Requests received from the Legacy Systems are passed to the Central system which then manages the transmission and collection of data to the meters. Responses received from the meters are received by the Central System and passed on to the correct Legacy System so that the relevant business process can be completed.

## 4.6 Local O&M Devices

Local O&M devices are portable devices used by DSO service personnel to locally configure, operate and maintain electronic devices that form part of the OPEN meter architecture. In Figure 1 three Local O&M components are defined:

- Local O&M device for Electricity Meter/Communication hub (MI3 interface).
- Local O&M device for Multi-utility meters (MUMI2 interface).
- Local O&M device for Concentrator (CI3 interface).

The O&M devices may include equipment such as laptops, hand-held PDA's, or dedicated monitoring and maintenance equipment. The devices are typically used during installation to configure the meter or Concentrator, and later to perform maintenance or reconfiguration where such functionality is not supported remotely by the Central System. The Local O&M device could also be used to retrieve meter data in the event of a sustained communications failure between the Central System and a particular meter or Concentrator.

Communication with the meter or Concentrator is typically via a connected cable or short-range wireless communications to the Local O&M device.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**29/83

## 4.7 Multi-utility meter

The multi-utility meter refers to an electronic smart-metering device that can measure a range of utility services such as gas, water and heat at the consumer's premises.

These meters are usually not connected to mains power i.e. they are typically battery powered. In terms of the OPEN meter architecture they are connected to the Electricity Meter/Communications Hub via interface MUMI1.

If the Electricity Meter/Communications hub is configured as a Gateway the Central System communicates directly with the multi-utility meter; if configured as a Proxy Gateway, the multi-utility meter communicates only with the Electricity Meter/Communications hub, and not directly with the Central System.

## 4.8 End Customer devices

End Customer devices are auxiliary equipment connected to the meter installation that enables the customer to interact with the electricity meter, multi-utility meters and/or load devices within the premises. Interaction with the customer is typically via a visual display interface that can be permanently mounted or portable.

The End Customer device is an optional device as it does not directly influence the functioning of the AMI system. However, in many cases an End Customer device, such as a consumption display unit, could help to influence customer behavior to support the AMI objectives. For example if the device is used to display electricity, gas, water or heat consumption together with current tariffs, customers may be prompted to utilize more energy efficient appliances, or use them at different times of the day. Advanced devices could also enable the consumer to manage the operation of specific loads from a single user interface, using the in-home network.

The End Customer device connects to the Electricity Meter/Communication hub via the MI5 interface.

## 4.9 External Devices

External Devices refer to (optional) equipment that is connected to the Concentrator and which utilize the smart metering communications infrastructure to support the AMI objectives. Examples include remote sensors or DER or SCADA systems installed in the same electrical substation as the Concentrator.

External devices can measure relevant data over the power system and relay this information to the Electricity meters or to the Central System. So for example, if a temporary overloading situation is detected at a substation, the information could be used by the Central System and/or the electricity meters to actively manage customer load in the short term to alleviate the problem.

The External devices are typically installed in a relatively short radius from the Concentrator, and will typically be mains powered. Connection with the Concentrator is via interface CI4, which could be wired or wireless interface.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**30/83

## 5 Interfaces

### 5.1 MI1-CI1

MI1-CI1 is the interface between the Electricity Meter/Communication Hub and the Concentrator.

MI1-CI1 conveys data and control information through PLC. Technologies considered in this document, PRIME and IEC 61334-5-1 (see Chapter 7 for a detailed description of the Protocol Architecture) operate in a similar “master-slave” way. Nevertheless, PRIME allows higher data rates and is better suited for supporting future applications than IEC 61334-5-1. In both cases, the Concentrator requests data from the electricity meters, and is responsible as well of maintaining and building up the network.

Note that electricity meters are directly managed by Concentrators through PLC via MI1-CI1. The Central System delegates these functions in the Concentrators (if present), but electricity meters may be additionally accessed and configured by the Central System, in case that interface MI2-SI2 is available. Direct management of electricity meters by Concentrators via interface MI1-CI1, where PLC technology is considered, is more robust and has a lower economic cost than via GPRS/UMTS, which are the technologies considered for interface MI2-SI2 (electricity meter – Central System).

See Chapter 7 for further information.

### 5.2 MI2-SI2

This is the interface for direct communications between the Electricity Meter/Communication Hub and the Central System, which obviously will usually take place through a public WAN network.

See Chapter 8 for further information.

### 5.3 MI3

This interface is the Local Operations & Maintenance interface of the electricity meters.

Its purpose is to provide a means for local parameterization during installation and to access meter data when the presence of a meter operator is required, for example the operation of physical security mechanisms, or when remote access is not possible for any reason.

In electricity metering the most common practice is to use an optical or current loop interface. The mechanical, optical and electrical characteristics of these are specified in IEC 62056-21. The protocol could be IEC 62056-21 Mode C or Mode E using the DLMS/COSEM 3-layer, HDLC based profile, or the TCP/IP based profile over PPP.

Another usual solution is to use an RS 232 or RS 485 interface, using the DLMS/COSEM 3-layer, HDLC based profile.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**31/83

In order to keep the installation costs at a minimum, local configuration should be prevented; auto configuration procedures should be used wherever possible.

See Chapter 9 for further information.

## 5.4 MUMI2

This interface is the Local Operations & Maintenance interface of the multi-utility (non-electricity) meters.

Its purpose is to provide a means for local parameterization during installation and to access meter data when the presence of a meter operator is required, for example the operation of physical security mechanisms, or when remote access is not possible for any reason.

For this interface many proprietary solutions exist today, using encoders, optical or inductive interfaces etc. with proprietary protocols.

A cost effective solution would be to use the MI3 interface of the Electricity Meter/Communication Hub to reach the multi-utility meters via the MUMI1-MI4 interface for operation and maintenance purposes.

Another important driver is cost: implementing different technologies for each interface would considerably increase the cost.

In order to keep the installation costs at a minimum, local configuration should be prevented; auto configuration procedures should be used wherever possible.

See Chapter 10 for further information.

## 5.5 MUMI1-MI4

This is the interface between the multi-utility meter and the Electricity Meter/Communications hub, which in OPEN meter is the only interface through which a multi-utility meter can ultimately communicate to an AMI Central System.

See Chapter 11 for further information.

## 5.6 MI5

This interface is not in the scope of further research inside WP3. It represents the link between a smart electricity meter and possible in-home, customer-owned devices for energy management and control. The ability to communicate to the Electricity Meter/Communications hub gives the End Customer device a link to external systems, also this way the utility could gain access or obtain information from customer premises.

See Chapter 12 for further information.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**32/83

## 5.7 CI2-SI1

This is the interface through which the Central System accesses all of its Concentrators. Usually a WAN interface which could be based on public or private networks, OPEN meter does not make an assumption on technologies used for lower layers for CI2-SI1. Just the requirement that an IP network exists is considered. GPRS/UMTS, fiber optics, Broadband PLC are all valid alternatives.

See Chapter 13 for further information.

## 5.8 CI3

The CI3 interface links the Concentrator with any O&M hardware. This interface is mainly dedicated to the local management, maintenance, operation and configuration of the Concentrator. O&M devices may assume some of the functionality of the Central System when the communication link between the Concentrator and the Central System is down, or when the Central System itself is out of order. In such cases, O&M devices may gather all the information from the Concentrator which is normally requested by the Central System: information related to smart metering, as well as the deliverance of configuration, control and operation commands to the Concentrator.

See Chapter 14 for further information.

## 5.9 CI4

The interface CI4 represents the communications interface between the metering data Concentrator, and any external device, such as sensors, that may require connection to it. These external devices are initially considered as small units close to the data Concentrator, within the same utility premises. The nature of the external devices has not been identified upfront, so this interface remains quite open for evolution in the future. Moreover this interface is not considered a core issue from the OPEN meter System Architecture perspective (see Figure 1).

As a result of this, interface CI4 will not be further analyzed within WP3.

This interface may be used for extensions to substation automation applications.

See Chapter 15 for further information.



Work Package: WP3

Type of document: Deliverable

Date: 08/02/2010

Energy Theme; Grant Agreement No 226369

Title: Design of the overall System Architecture

Version: 1.1

Page:33/83

## PART II – Communication Profiles for Open Meter System Interfaces

### 6 Security

#### 6.1 Security needs

Security requirements are considered as a critical element and have been identified in [1] (§3.2.1.2). They take into account the needs for access and use control, data integrity, data confidentiality and resource availability. They concern both modules and interfaces.

Table 4 – Overview of Security requirements

Function category	Security need	Description	D1.1 Reference
Minimum	Access and Use Control	The system must be capable of authenticating entities	OM-GR2
	Access and Use Control	The system must be capable of managing access rights for any of its components	OM-GR3
	Data integrity	The system must be capable of guaranteeing the integrity of data exchanged	OM-GR4
	Data Confidentiality	The equipment shall provide functionality to preserve the confidentiality of data storage	OM-GR5
	Data integrity	The equipment shall provide functionality to preserve the integrity of data storage, including integrity of equipment firmware	OM-GR6
	Data Confidentiality	The system and devices should provide functionality to prevent eavesdropping	OM-GR7
	Data integrity	The system will be capable of implementing an anti-replay mechanism	OM-GR8
	Access and Use Control Data integrity	Broadcast communication shall take place in a secure manner	OM-GR9
	Access and Use Control Data integrity Data Confidentiality	The equipment shall provide functionality for management of encryption keys	OM-GR11
	Access and Use Control Data integrity	Physical access to devices should be made difficult	OM-GR12
	Access and Use Control Data integrity Data Confidentiality	Respecting standards developed for IT technologies and Automation systems should be the best way to implement secured AMI systems	OM-GR15
	Access and Use Control Data integrity Data Confidentiality	Usage of "certificates" to enable security features is strongly recommended	OM-GR16
	Resource Availability	All parts of the network must be under control, supervision and administration.	OM-GR17
Advanced	Resource Availability	A supervision of system behaviour should be possible, abnormal situations detected, and some automatic corresponding actions should be possible	OM-GR10
	Access and Use Control Data integrity	Attempting to access a local maintenance port of device will be logged	OM-GR14
Optional	Access and Use Control	All unused device physical interface (about gateway, data Concentrator, meter) will be disabled by default	OM-GR13

As the mechanisms that are necessary to fulfil these requirements in the modules are most often implementation and organization dependent, the requirements above complemented with their fit criteria given in [1] will be regarded as sufficient, and won't be developed further.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**34/83

For the interfaces there is a need to give further details about mechanisms and security features available with the communication protocols and that need to be implemented, at least for interoperability purposes. Sections 6.2 and 6.3 deal with communications security for the interfaces.

## 6.2 Security features of DLMS/COSEM

### 6.2.1 Introduction

DLMS/COSEM provides two main information security features for accessing and transporting data:

- *Data access security* controls access to the data held by a DLMS/COSEM server, see 6.2.2;
- *Data transport security* allows the sending party to apply cryptographic protection to the xDLMS APDUs sent. This requires ciphered APDUs. The receiving party can remove or check this protection; see 6.2.3.

These information security features are provided partly by the COSEM Application layer, partly by COSEM objects:

- Upon AA establishment, two contexts are negotiated using the ACSE services: the *application context* and the *authentication context*. The application context determines whether ciphered APDUs can be used or not. The authentication context determines the level of data access security. The ACSE APDUs are not cryptographically protected;

*NOTE : The ACSE APDUs may carry cryptographically protected association information.*

- Once an AA is successfully established, COSEM services can be used to access attributes and methods of COSEM objects, depending on the access rights valid for the given association. These services are carried by xDLMS APDUs, which may be cryptographically protected: authenticated, encrypted, or both, depending on the security context in force. The cryptographic protection is applied, removed or checked by the COSEM Application layer. The COSEM AP of the sending party informs, via service parameters, the COSEM AL about the protection to be applied to the APDU to be sent. The COSEM Application layer of the receiving party informs the COSEM AP about the protection that has been applied to the APDU received.

The message security methods described in this document have been selected from the standards specified by NIST and the IETF.

### 6.2.2 Data access security

Data access security concerns role based access to data in a DLMS/COSEM device.

It is managed by the Association LN (Logical Name) / Association SN (Short Name) objects. Each COSEM server (i.e. a logical device) may support AAs with various clients, each having a different role, and with this, different access rights. Each AA is identified with a pair of lower layer addresses. Each Association object provides a list of



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**35/83

objects visible in that particular AA and the access rights to their attributes and methods.

To be able to access data, the client must be properly authenticated. Upon AA establishment, an authentication context is negotiated between the client and the server. This specifies the required authentication of the peers, and, where needed, the security algorithm to verify the authentication. Three data access security levels are provided:

- Lowest level security (no security);
- Low Level Security (LLS);
- High Level Security (HLS).

The purpose of lowest level security is to allow the client to retrieve some basic information. This authentication context does not require any peer authentication; it allows direct access to the data in the server, within the access rights available in the given AA.

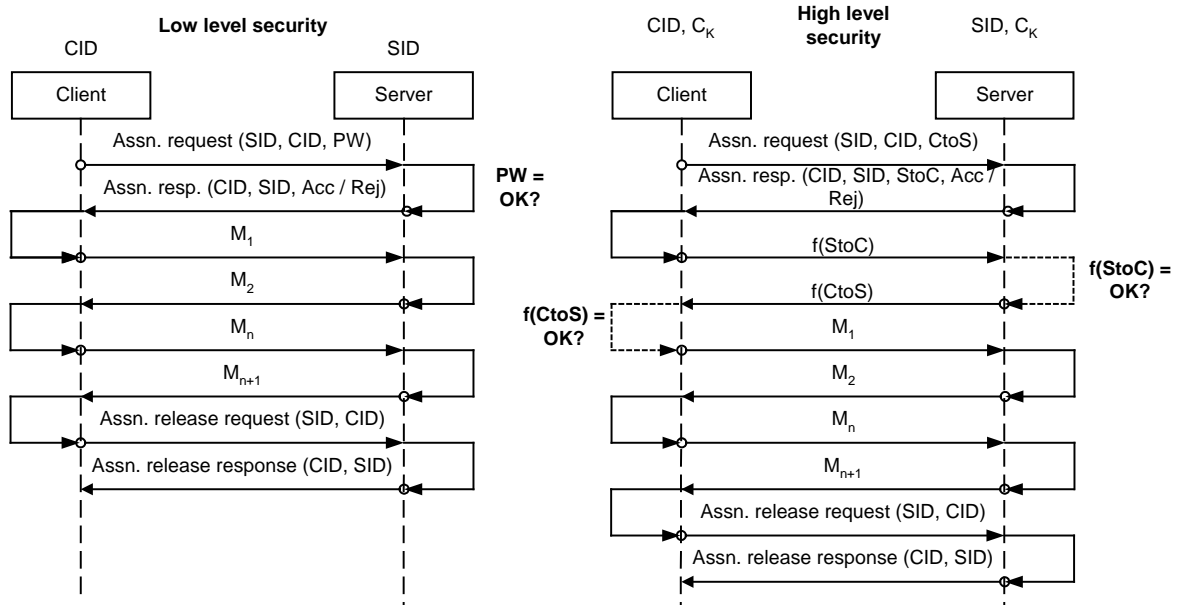
The purpose of LLS is to allow the authentication of clients by verifying the password supplied. The server is not authenticated. This authentication context is typically used when the communication channel offers adequate security to avoid eavesdropping and message (password) replay.

The purpose of HLS is to allow mutual authentication of the client and the server participating in an association. This authentication context is typically used when the communication channel offers no intrinsic security and precautions have to be taken against eavesdroppers and against message (password) replay.

HLS requires that both the client and the server mutually authenticate each other. This is a 4-step process, involving the exchange of challenges during AA establishment, which is followed by exchanging the results of processing these challenges, using cryptographic methods. If the authentication takes place, the client can proceed to access data within the access rights available in the given AA, and it accepts data coming from the server. Otherwise, the AA is not established.



**Energy Theme; Grant Agreement No 226369**



CID: Client address, SID: Server address, PW: Password,  $C_K$ : shared secret, CtoS: client challenge to server, StoC: server challenge to client

Figure 3 – LLS and HLS authentication

**6.2.3 Data transport security**

**6.2.3.1 Applying, removing or checking the protection: ciphering and deciphering**

For data transport security, cryptographic protection can be applied before sending an xDLMS APDU – as determined by the security policy, see 6.2.3.3 – then removed or checked after the reception of an APDU.

*NOTE: ACSE APDUs are not cryptographically protected.*

*NOTE: Cryptographic protection of data in storage is out of the Scope of this document.*

Applying the protection is achieved by ciphering. Deciphering removes or checks the protection, restoring the original xDLMS APDU. Ciphering and deciphering is performed by the COSEM Application layer as shown in Figure 4.

When a COSEM service request or response primitive is invoked by the client or the server AP respectively, the service parameters include the Security\_Options parameter. This parameter informs the Application layer on the requested security to be applied on the xDLMS APDU carrying the service primitive, and it may identify elements of the security material to be used.

Similarly, a COSEM service indication or confirm primitive includes a Security\_Status parameter. This parameter informs the AP on the security that was applied on the xDLMS APDU carrying the service primitive, and it may include information on the elements of the security materials used. The authentication tag, if any, is also passed.

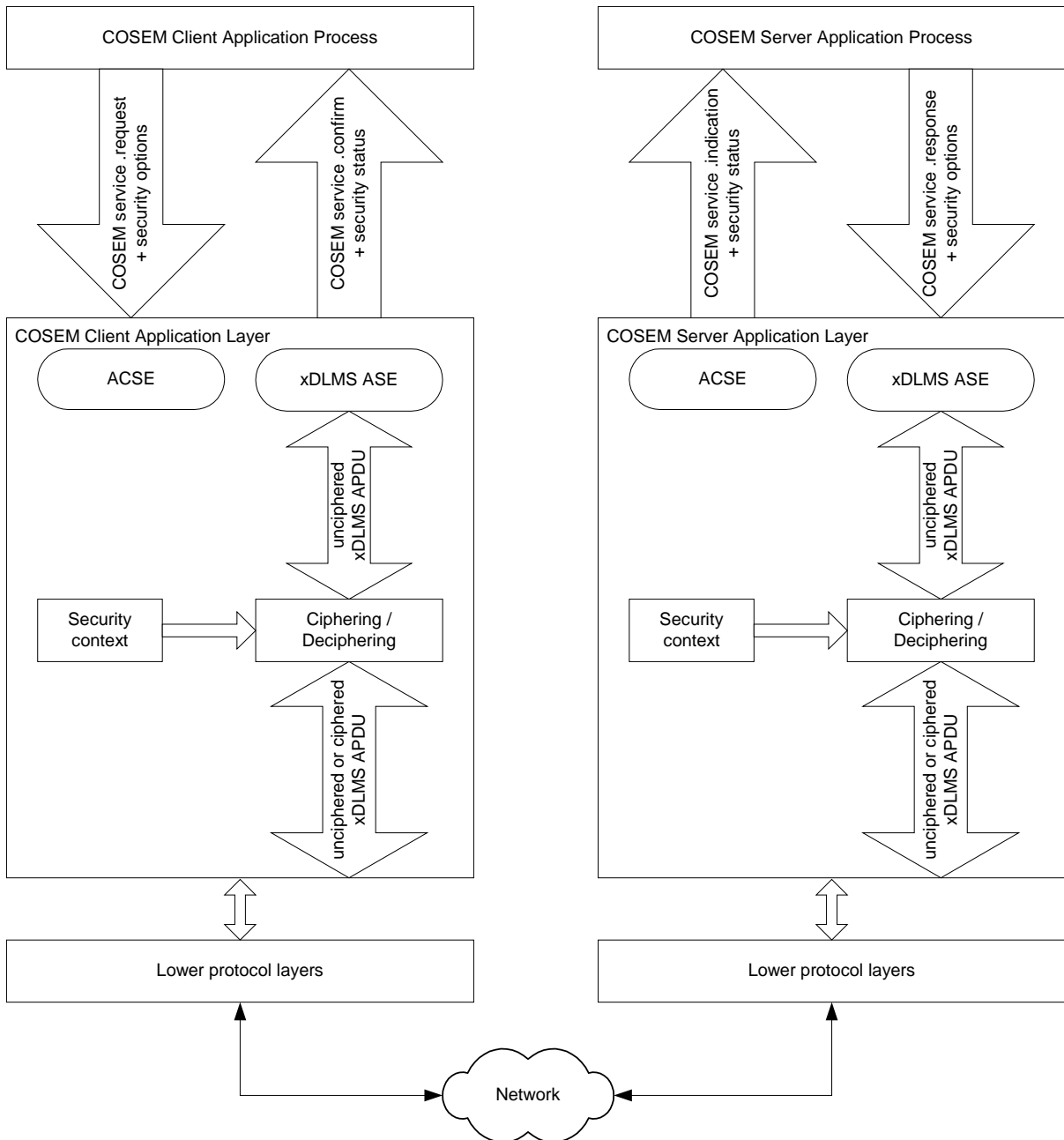


Figure 4 – Data transport security in DLMS/COSEM

### 6.2.3.2 Security context

The security context defines security attributes relevant for the ciphering / deciphering process:

- The security policy in force, determining the kind of protection to be applied. See 6.2.3.3;
- The security suite, specifying the security algorithm(s). See 6.2.3.4;



**Energy Theme; Grant Agreement No 226369**

- The security material relevant for the given security suite, including elements like block cipher keys, authentication keys, initialization vectors etc. See 6.2.3.5.

**6.2.3.3 Security policy**

The following security policies are specified:

- Security is not imposed;
- All messages authenticated;
- All messages encrypted;
- All messages authenticated and encrypted.

The security policy is held by the security\_policy attribute of the Security setup object.

Authenticated access may be required selectively: certain attributes and methods may be accessible only by using authenticated messages. This is indicated by the access mode to each attribute and method. Therefore, authenticated xDLMS APDUs may be used – within a ciphered application context – even when the security policy in effect does not require that all messages be authenticated.

Note that if authenticated access is required, but the application context is not a ciphered one, the attributes and methods requiring authentication cannot be accessed. If the client attempts to send a ciphered APDU in an unciphered application context, then the server application layer shall reject it. In the case of SN referencing, the response shall be ConfirmedServiceError APDU, carrying the tag of the rejected APDU. In the case of LN referencing, the response shall be an EXCEPTION.response APDU.

On the other hand, encryption applies generally for all messages within a given AA: if the security policy requires that all messages shall be encrypted, then all APDUs shall be encrypted – and additionally they may be authenticated.

When the security policy requires that all messages shall be authenticated and encrypted, then only APDUs that are both encrypted and authenticated can be used.

Messages protected by higher security than what the security policy requires are always allowed (provided that the application context negotiated allows them).

**6.2.3.4 Security suite**

A security suite determines the cryptographic algorithm(s) used for message security. A security suite is identified with a Security Suite ID; see Table 5. Currently, one security suite is specified, the Galois/Counter Mode (GCM) with AES-128 (see [6]). In this security suite, global keys are protected during transportation using the AES-128 key wrap algorithm.

*NOTE : Other security suites may be added later.*

Table 5 – Security suites

Security Suite Id	Authentication algorithm	Encryption algorithm	Key transport method
0	AES-GCM-128	AES-GCM-128	Key wrapping using AES-128 key wrap
All other reserved	–	–	–



**Energy Theme; Grant Agreement No 226369**

**6.2.3.5 Security material**

The elements of the security material are the following:

- A block cipher key, denoted *EK*;
- An authentication key, denoted *AK*;
- An initialization vector, denoted *IV*;
- Message to be secured, denoted *M*.

The first three elements depend on the security suite. For AES-GCM-128, they are defined in [5]. The message to be secured is the unciphered xDLMS APDU.

**6.2.3.6 Ciphered xDLMS APDUs**

Ciphered xDLMS APDUs can be used in a ciphered COSEM application context only. A ciphered APDU is always an octet string.

*NOTE : In a ciphered COSEM application context, unciphered APDUs may also be used.*

The structure of the ciphered APDU depends on the kind of ciphering applied; see Figure 5:

- If the APDU is authenticated only, it contains the APDU tag, the length field, the security header field, the original APDU and the authentication tag;
- If the APDU is encrypted only, it contains the APDU tag, the length field, the security header field, and the encrypted DLMS APDU;
- If the APDU is both authenticated and encrypted, it contains the APDU tag, the length field, the security header field, the encrypted APDU and the authentication tag.

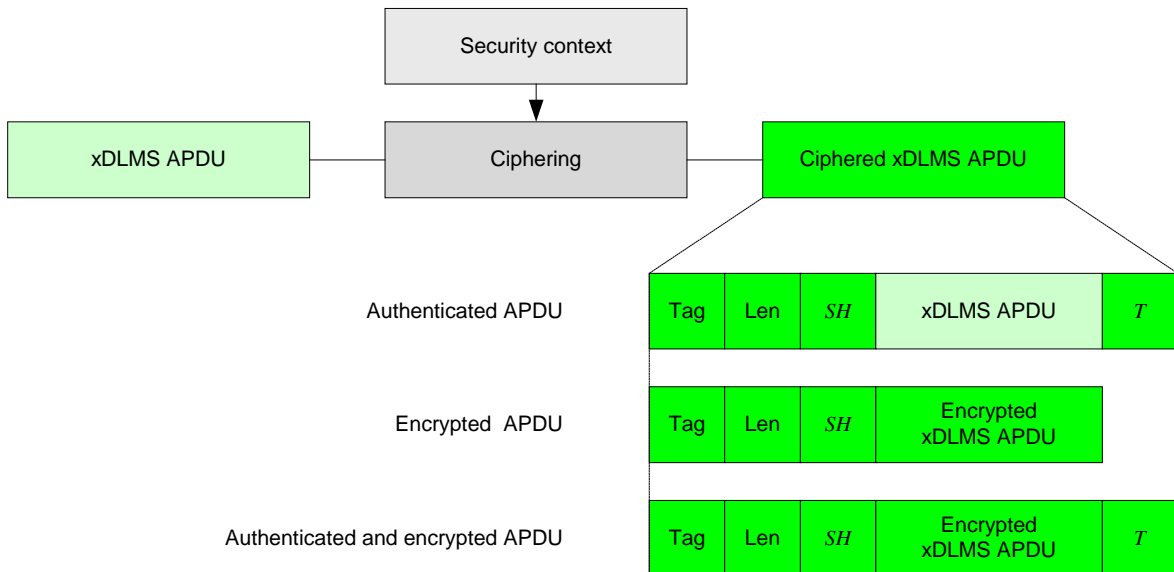


Figure 5 – Ciphered xDLMS APDUs

The APDU tag identifies the type of the APDU.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**40/83

The length field specifies the length of the octet-string.

The Security Header, *SH*, includes the Security Control field, *SC* right concatenated with the Frame Counter, *FC*.

The security control field is shown in Table 6, where:

- Bit 3...0: Security\_Suite\_Id, see 6.2.3.4;
- Bit 4: "A" subfield: indicates that the APDU is authenticated;
- Bit 5: "E" subfield: indicates that the APDU is encrypted;
- Bit 6: Key\_set subfield (0=Unicast, 1=Broadcast);
- Bit 7: Reserved, must be set to 0.

Table 6 – Security control byte

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3...0
Reserved, set to 0	Key_set	E	A	Security_Suite_Id

The Frame Counter is an internal counter maintained by the sending and receiving parties.

Finally, *T* is the authentication tag, calculated by the authentication algorithm.

### 6.3 Security in lower layers

Almost all the communication profiles described in OPEN Meter implement DLMS/COSEM as upper layers. DLMS/COSEM security features described above in 6.2, deal mainly with authentication and confidentiality, and thus allow fulfilling part of the security requirements given in [1], on the interfaces transporting DLMS/COSEM messages.

Nevertheless in some cases it might be desirable to implement other security mechanisms which may already exist in other protocols used in conjunction with DLMS/COSEM in a communication profile. Some could be of better strength or efficiency, or would allow extending security to elements that are not part of the application data when they need to be also protected (for instance network addresses).

Detailed technical recommendations for security will be given for each communication profile in further next WP3 Tasks.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**41/83

## **7 MI1-CI1 (Electricity Meter/Communication hub-Concentrator)**

### **7.1 Introduction**

This interface is between the Electricity Meter/Communication hub, and the Concentrator, located, for example, in an electrical MV/LV substation.

The Protocol Architecture is shown in Figure 6.



**Energy Theme; Grant Agreement No 226369**

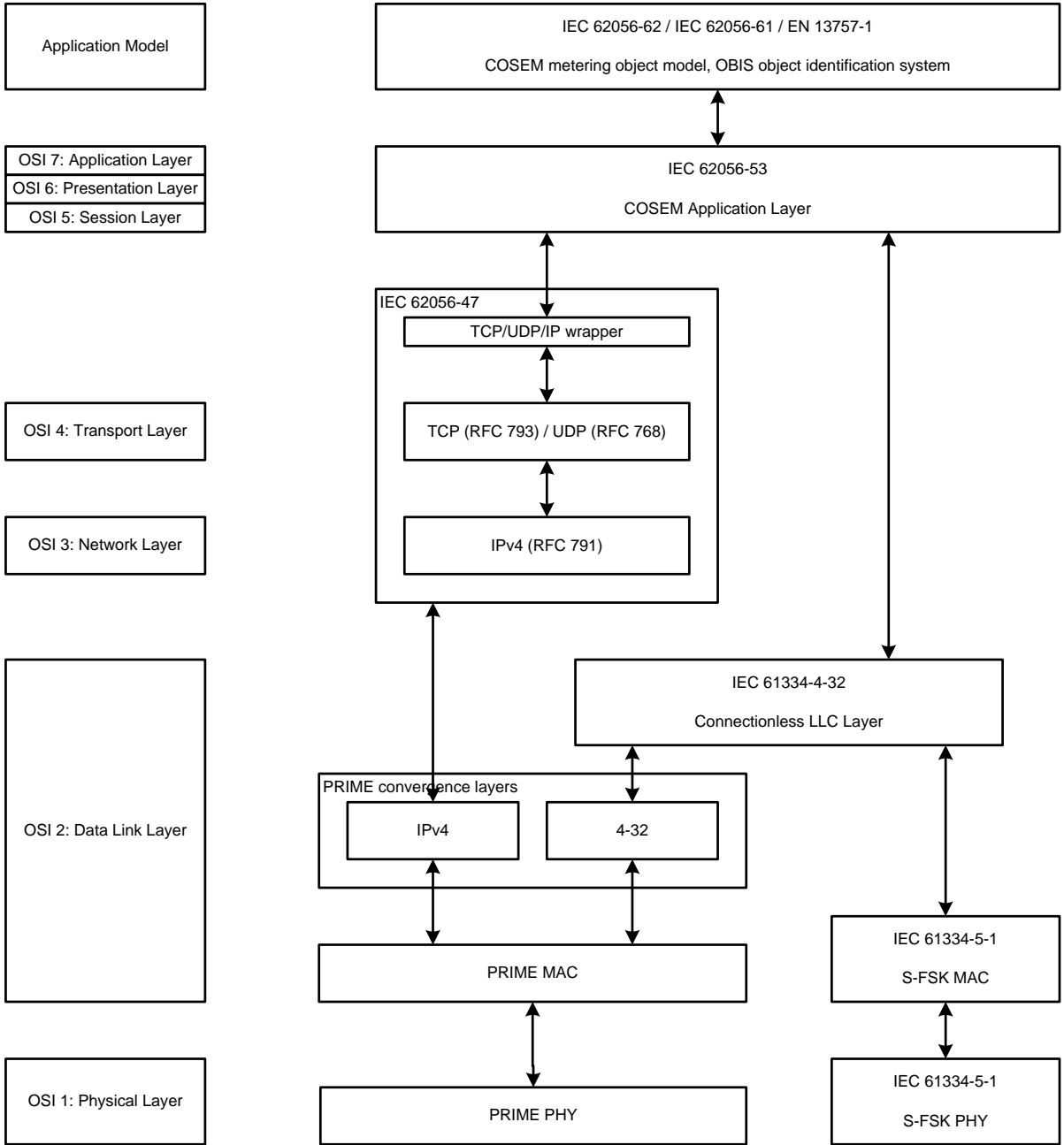


Figure 6 - MI1-CI1 architecture

For this interface, two PLC technologies, both working in the CENELEC A Band have been selected:

- IEC 61334-5-1 S-FSK (see [7]);
- PRIME (see [8]).

The following sections will describe each one briefly.



## 7.2 Architecture of the DLMS/COSEM S-FSK PLC profile

A more detailed architecture is shown in Figure 7.

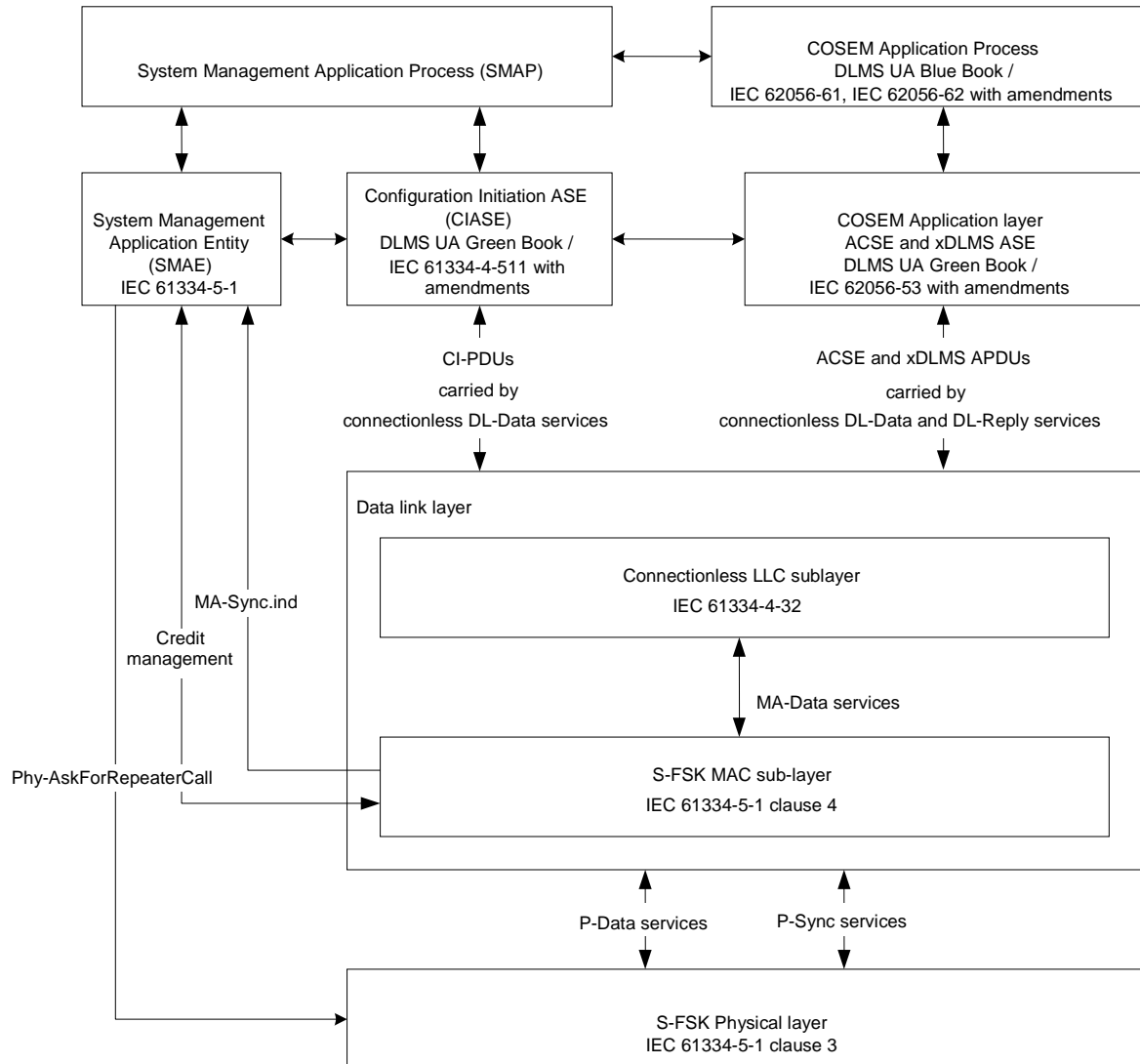


Figure 7 - DLMS/COSEM S-FSK PLC architecture

This protocol stack uses three-layer collapsed OSI model:

- The Application layer, covering the Application, Presentation and Session functionalities;
- The Data link layer, that consists of the MAC layer and the LLC layer;
- The Physical layer.

### 7.2.1 Physical layer

The PHY provides the interface between the equipment and the physical transmission medium that is the distribution network. It transports binary information from the source to the destination.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**44/83

The PHY in this profile is as specified in [7] (§3). It provides the following services to its service user MAC sublayer:

- P-Data services to transfer MPDUs to (a) peer MAC sublayer entity(ies) using the LV distribution network as the transport medium;
- P-Sync services to allow the MAC sublayer entity to ask for a new synchronization and to be informed of a change in the synchronization state of the PL. These services are used locally by the MAC sublayer.

See [7] (§3.4).

### **7.2.2 Data Link layer**

The data link layer consists of two sublayers: the Medium Access Control (MAC) and the Logical Link Control (LLC) sublayer.

The MAC sublayer handles access to the physical medium and provides physical device addressing.

The decision to access the medium is made by the initiator, directly for its own MAC sublayer or indirectly for other MAC sublayers which are requested to transmit a response to a request sent previously by the initiator.

The LLC sublayer controls the logical links. OPEN meter considers the use of the connectionless LLC sublayer, as specified in [9].

#### **7.2.2.1 The MAC sublayer**

The MAC sublayer of the DLMS/COSEM S-FSK PLC communication profile is as specified in [7] (§4). It provides the following services to its service user LLC sublayer:

- The MA-Data services. These services allow the LLC sublayer entity to exchange LLC data units with peer LLC sublayer entities. See [7] (§4.1.3.1);
- The MA-Sync.indication service. This allows the SMAE entity to be informed of the synchronization and configuration status of the device. See [7] (§4.1.3.2).

#### **7.2.2.2 The connectionless LLC sublayer**

The connectionless LLC sublayer is as specified in [9]. It is derived from [10] - similar to Class III operation - and it performs the following functions:

- Addressing of application entities within the equipment;
- Sending data with no acknowledgement (SDN);
- Requesting data with reply (RDR).

It provides the following services:

- DL-Data services for transporting CI-PDUs, ACSE APDUs and client-server type xDLMS APDUs;
- DL-Reply services for asking the remote LLC sublayer entity to send a previously prepared LSDU;
- DL-Update-Reply services to prepare the LSDUs to be transferred using the DL-Reply services.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**45/83

For additional information, see [9] (§2.1).

### **7.2.3 Networking Layers (Network, Transport)**

No network layer, neither transport layer, are defined for this S-FSK DLMS/COSEM PLC profile.

### **7.2.4 Upper layers (Session, Presentation, Application)**

The application layer is the COSEM Application layer as specified in [11]. It provides services to the COSEM application process (AP) and uses the services of the connectionless LLC sublayer.

The AL contains two main Application Service Elements:

- The Association Control Service Element, ACSE;
- The xDLMS ASE.

The task of ACSE is to establish, maintain, and release application associations. For the purposes of DLMS/COSEM CO communication profiles, the CO ACSE specified in [12] and [13] is used.

The task of the xDLMS\_ASE is to provide data transfer services between COSEM APs. It is based on the DLMS standard, [14]. It has been extended for DLMS/COSEM; see [5]. The main objective of the DLMS/COSEM approach is to provide a business domain oriented interface object model for metering devices and systems while keeping backward compatibility to the DLMS standard. To meet these objectives, DLMS/COSEM includes an evolution of DLMS. Remaining fully compliant to the DLMS standard, DLMS/COSEM provides a more metering-specific view of the meter through the COSEM interface objects.

### **7.2.5 Data Model**

As specified in [15], COSEM models metering equipment as a single physical device containing/hosting a set of one or more logical devices. Each logical device models a subset of the functionality of the metering equipment as these are seen through its communication interfaces.

Each physical device should have its own physical and MAC address on the network, which can be assigned during manufacturing (static address), or during registration on the network (dynamic address).

The logical device(s) hold the various parameters and measurement data. Using more than one logical device may be useful to organize data and the access to them. For example, a gas meter may have a management logical device to hold parameters and a gas logical device to hold the measurement data. In simpler devices, only the management logical device may be present, holding all data.

Each logical device (LD) can be seen as an application process (AP), using the services of the COSEM application layer, and each LD is bound to an address in the protocol layer supporting the COSEM application layer.

The functionality of each logical device is modeled by the COSEM interface objects - instances of COSEM interface classes - implemented in them. The COSEM interface classes are specified in [15]. Their naming system - the OBIS codes - is specified in [16].

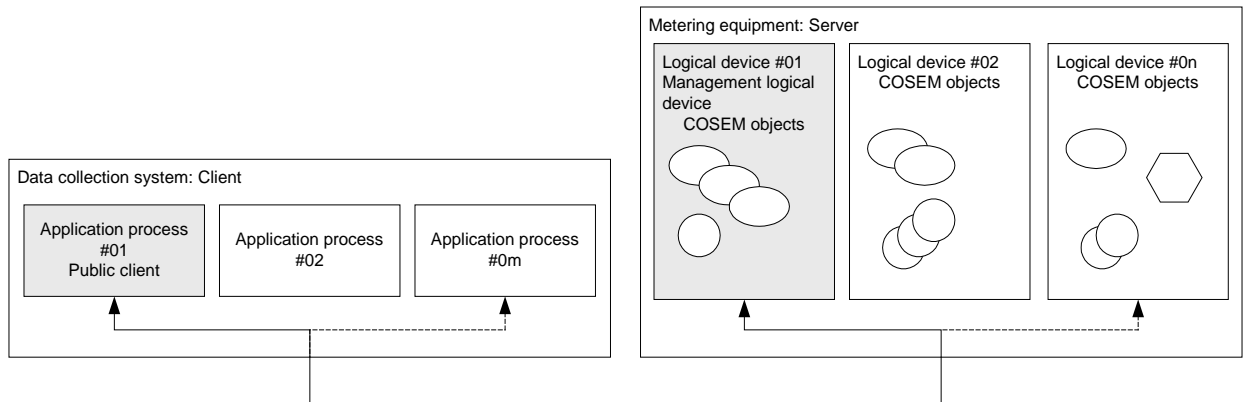


Figure 8 - COSEM application model of a Concentrator and metering equipment

Concentrators are modeled as a set of APs. Each AP may have different roles and access rights, granted by the metering equipment.

*NOTE: The application processes may be hosted by one or several physical devices.*

The Public client and the Management logical device APs have a special role and they must always be present. See more in Chapter “COSEM interface classes” in [17].

Some examples of COSEM objects are:

- Data, Register, Extended register and Demand register objects to hold measurement values like energy, demand, flow, index, voltage, current, pressure, temperature, and also parameters;
- Profile generic objects to hold series of data, like load profiles or billing data;
- Clock, Schedule, Activity calendar, Register monitor, Limiter and Script objects to manage time and event bound activities;
- Association objects, to control role based access to the resources of the meter;
- Security setup objects,
- Image transfer object to manage downloading a new firmware;
- Communication layer setup objects.

The Central System, the Concentrator and the local O&M devices could act as clients for the meters which are playing the role of servers (cases of interfaces MI2-SI2, MI1-C11 and MI3 respectively). The client requests services from the servers which provide them.

Each client has a specific role, and the server provides access to its resources according to that role. This is controlled by the Association objects.

On the client side, more than one Application Process may exist, for example Management, Electricity meter reader, Gas meter reader, Utility engineer, Manufacturer. The client application processes make use of the resources of the server APs, by accessing attributes and methods of COSEM objects. Attributes can be read



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**47/83

and written and methods can be invoked as specified by the access rights in a given Application Association.

### 7.2.6 Security

Briefly, in DLMS/COSEM there are several mechanisms which are in charge of providing various levels of security to the information exchange. Some of these mechanisms have to do with the logical representation of the data structure of the devices: different logical devices can have a number of access constraints, being different between them. Thus, the definition of several logical devices, each of them with its own access level, passwords and criteria and its own subset of objects, having each of them its own read-write access constraints, may give a high degree of security when attempting to access to any of the objects that constitute the complete logical image of the device.

In general, we can distinguish different security mechanisms:

- Access requisites and selective access: providing control access to data. These mechanisms are made available by the COSEM AL and the interface objects (Association object). The access level (not protected at all, password-protected or even APDU encryption) can be negotiated upon association establishment. The same can be done also for the access services allowed for each logical device, say: GET, SET, ACTION procedures. This, with the addition of the control of the type of access allowed for each of the attributes of the objects that constitute the logical device, provides a level of security.
- High Level Security (HLS): an authentication mechanism used to establish the true identity of both the client and the server. High Level Security authentication is typically used when the communication channel offers no intrinsic security and precautions have to be taken against eavesdroppers and against message (password) replay.
- Low Level Security (LLS): an authentication mechanism used to establish the true identity of the client by verifying a password. Low Level Security is used when the communication channel provides adequate security to avoid eavesdropping and message (password) replay. The password is a piece of information held by the server and submitted by the client when the LLS authentication mechanism is used. It is carried by the Calling/Responding\_Authentication\_Value parameter of the COSEM-OPEN service.

See the DLMS documentation referenced in this document for further information.



### 7.3 Architecture of the DLMS/COSEM PRIME PLC profile

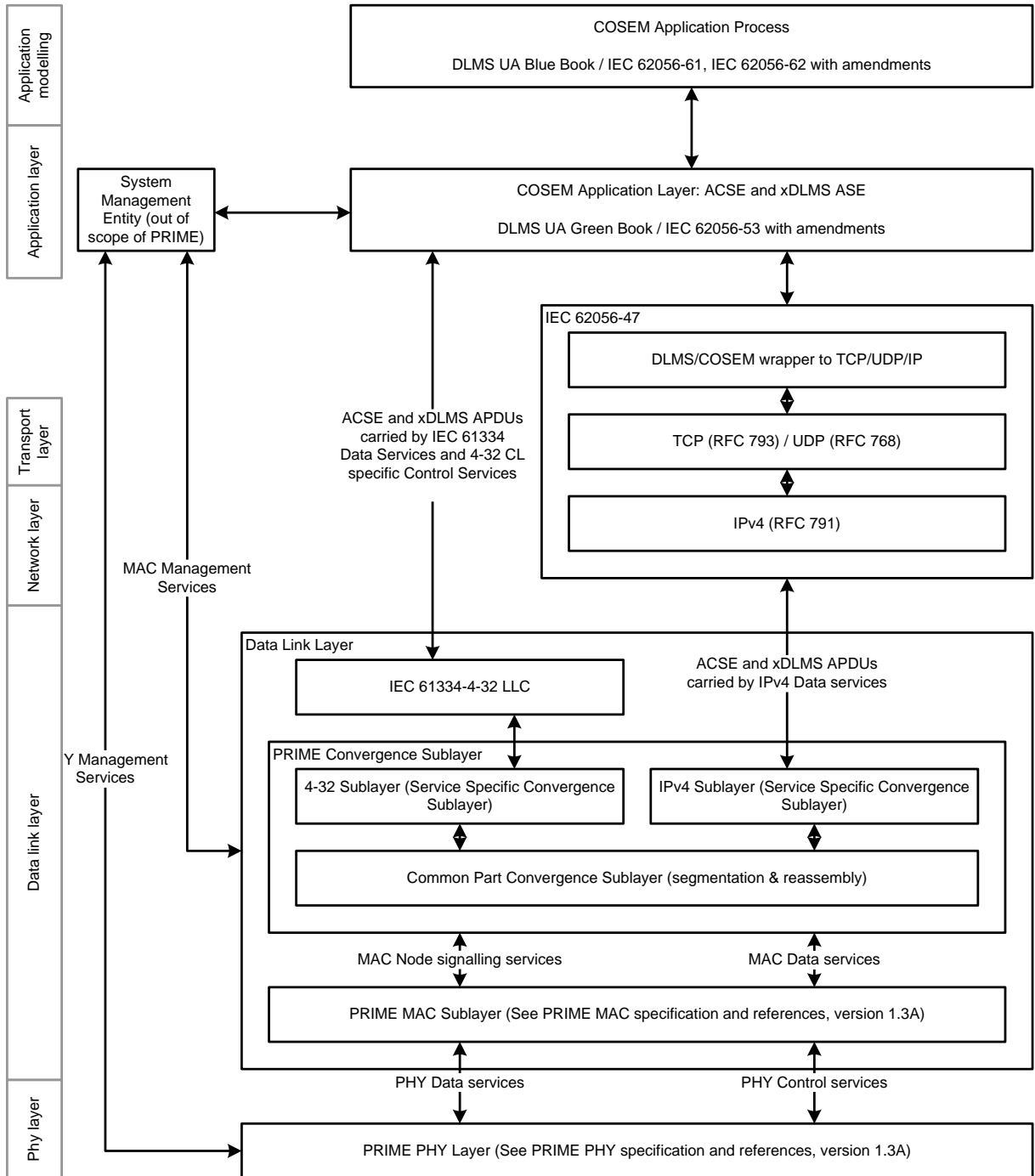


Figure 9 - DLMS/COSEM PRIME PLC architecture

The proposed protocol stack uses the following OSI layers:

- The Application layer, covering the Application, Presentation and Session functionalities;



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**49/83

- The IP Network layer and the TCP Transport layer, only for the IPv4 profile over PRIME, plus the TCP/IP wrapper to DLMS/COSEM.
- The PRIME Data link layer, that consists of the MAC layer and the CPCS and the corresponding SSCS, according to the selected profile (4-32 or IPv4);
- The PRIME Physical layer.

### 7.3.1 Physical Layer

#### 7.3.1.1 Introduction

As stated in the section related to the PHY for the S-FSK profile, this layer provides the interface between the equipment and the physical transmission medium that is the distribution network. This PHY transmits and receives MPDUs between neighbor nodes. The PRIME PHY consists on an OFDM system using the CENELEC A-band as defined in [18]. This comprises 3 kHz up to 95 kHz and is restricted to electricity suppliers and their licensees. The OFDM signal uses a frequency bandwidth of 47.363 kHz located on the high frequencies of CENELEC A-Band.

The OFDM signal itself uses 97 (96 data plus one pilot) equally spaced subcarriers with a short cyclic prefix. Differential modulation schemes are used, together with three possible constellations: DBPSK, DQPSK or D8PSK. An additive scrambler is used to avoid the occurrence of long sequences of identical bits, and finally,  $\frac{1}{2}$  rate convolutional coding is used along with interleaving. This can be disabled by higher layers if the channel is good enough and higher throughputs are needed.

#### 7.3.1.2 PRIME PHY data plane services

PHY DATA: generated by the MAC layer entity whenever data is to be transmitted to a peer MAC entity or entities, and passed to the PHY entity to request the sending of a PPDU to one or more remote PHY using the PHY transmission procedures. It also allows setting the time at which the transmission must be started. There are local primitives in charge of notifying the local MAC layer that a transmission procedure has been executed, successfully or not. Finally, there are primitives to indicate the arrival of a valid PPDU.

#### 7.3.1.3 PRIME PHY control plane services

PHY AGC: generated by the MAC layer entity and passed to the PHY entity to set, or to get, the Automatic Gain Mode of the PHY.

PHY TIMER: generated by the MAC layer entity and passed to the PHY entity to get the time at which the transmission has to be started.

PHY CD: generated by the MAC layer entity and passed to the PHY entity to look for the carrier detect signal, in order to detect if the physical medium is free.

PHY NL: generated by the MAC layer entity and passed to the PHY entity to get the floor noise level value present in the power line.

PHY SNR: generated by the MAC layer entity and passed to the PHY entity to get the value of the signal-to-noise ratio, in order to find the appropriate degree of robustness needed for data exchange.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**50/83

PHY RQ: generated by the MAC layer entity and passed to the PHY entity to get the value of the last received frame quality, in order to find the appropriate degree of robustness needed for data exchange.

PHY ZCT: generated by the MAC layer entity and passed to the PHY entity to get the zero cross time of the mains and the time between the last transmission or reception and the zero cross of the mains.

#### **7.3.1.4 PRIME PHY management plane services**

PLME RESET: invoked to request the PHY layer to reset its present functional state. As a result of this primitive, the PHY should reset all internal states and flush all buffers to clear any queued receive or transmit data.

PLME SLEEP: invoked to request the PHY layer to suspend its present activities including all reception functions. The PHY layer should complete any pending transmission before entering into a sleep state.

PLME RESUME: invoked to request the PHY layer to resume its suspended activities. As a result of this primitive, the PHY layer should start its normal transmission and reception functions.

PLME TESTMODE: invoked to enter the PHY layer into some non-default functional modes. Specific functional mode out of the various possible modes is provided as an input parameter. Following receipt of this primitive, the PHY layer should complete any pending transmissions in its buffer before entering the requested test mode.

PLME GET: invoked to query information about a given attribute of the PRIME Information Base.

### **7.3.2 Data Link Layer**

#### **7.3.2.1 MAC layer's main facts and functions**

##### *7.3.2.1.1 Introduction*

A subnetwork is a tree with two types of nodes, the Base Node and Service Nodes. The Base Node is at the root of the tree and acts as master node that provides the subnetwork with connectivity. It manages the subnetwork resources and connections. There is only one Base Node in a subnetwork. This Base Node is initially the subnetwork itself and other nodes should follow a registration process to enroll them on the subnetwork. Any other subnetwork node is a Service Node. Service Nodes are either leaves or branch points of the tree. These nodes start in a disconnected state and try to find a Base Node or any other Switch Node to establish network connectivity. Each of these nodes is one point of the subnetwork. These nodes have two responsibilities: connecting themselves to the subnetwork, and switching their neighbors' data to propagate connectivity.

Service Nodes change their behavior dynamically from "Terminal" functions to "Switch" functions and vice-versa. The changing of functional states occurs on the basis of certain pre-defined events on the network.

The three functional states of a Service Node as defined in the specification are:

**Disconnected**, all nodes are in this state when starting the network or after a node restart. In this state a node is not capable of communicating or switching the traffic of



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**51/83

another node. The primary function of a Service Node in this state is to search for an operational network in its proximity and try to register itself on it.

**Terminal:** In this state a Service Node is capable of communicating its traffic by establishing connections, but it is not capable of switching the traffic of any other node.

And finally **Switch:** In this state a Service Node is capable of performing all Terminal functions. Additionally, it is capable of forwarding data to and from other devices on the subnetwork. It is a branch point on the tree. The events and associated processes that trigger changes from one functional state to another are basically registration, unregistration, promotion and demotion. For further details see [8].

Other functions that fall into the MAC layer specification are:

- Address resolution and broadcast and multicast addressing.
- CSMA/CA algorithm implementation.
- Service Nodes functionality as Switches: promotion, demotion.
- Capability of establishing direct connections from one Service Node to another.
- Packet aggregation.
- Security issues, as encryption and security keys management.
- PHY robustness management in order to select the best modulation schema for a given situation.
- ARQ mechanism.

#### *7.3.2.1.2 Services for Base and Service Node signaling*

- MAC ESTABLISH: used to manage the connection establishment at MAC layer.
- MAC RELEASE: used to release a connection at MAC layer.
- MAC JOIN: used to join a broadcast or a multicast connection and to allow the reception of such packets.
- MAC LEAVE: used to leave a broadcast or a multicast connection.

#### *7.3.2.1.3 Services for Base Node signaling*

- MAC REDIRECT: used to answer to a MAC\_ESTABLISH.indication primitive. It also redirects the connection from the Base Node to another Service Node on the subnetwork.

#### *7.3.2.1.4 Services for Base and Service Nodes*

- MAC DATA: used to initiate the transmission process of unicast data over a connection, or to indicate that unicast data has arrived.
- MAC SEND: used to initiate the transmission process of multicast or broadcast data.

#### *7.3.2.1.5 Optional services: management entity*

- MLME REGISTER: used to perform registration and to indicate when registration has been performed.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**52/83

- MLME UNREGISTER: used to perform deregistration and to indicate when deregistration has been performed.
- MLME PROMOTE: used to perform promotion and to indicate when promotion has been performed.
- MLME DEMOTE: used to perform demotion and to indicate when demotion has been performed.
- MLME RESET: used to reset the MAC into a known good status.
- MLME GET: used to retrieve individual values from the MAC, such as statistics.
- MLME LISTGET: used to retrieve a list of values from the MAC.
- MLME SET: used to set configuration values in the MAC.

### 7.3.3 Convergence layers

The convergence layer is separated into two sublayers. The Common Part Convergence Sublayer (CPCS) provides a set of generic services. The Service Specific Convergence Sublayer (SSCS) contains services that are specific to one application layer. There are several SSCS, typically one per application, but only one common part. The use of the common part services is optional in that a specific service sublayer will configure into its protocol stack services which are required from the common part, and omit services that are not required.

At this moment, the CPCS provides the following service to the different SSCS: segmentation and reassembly.

Finally, PRIME provides two different, separate, SSCS to connect the MAC layer to the upper layer:

- The IEC 61334-4-32 LLC Convergence Layer
- The IPv4 Convergence Layer.

#### 7.3.3.1 The IEC 61334-4-32 LLC Convergence Layer

This convergence sublayer (SSCS) supports the same primitives as [9]. [19] should also be referenced for definitions of the destination address. The 4-32 SSCS provides convergence functions for applications that use IEC 61334-4-32 services. Implementations conforming to this SSCS shall offer all LLC services specified in [9] (§2). Additionally, the PRIME 4-32 SSCS provides extra services that help mapping the connection-less protocol to the connection-oriented nature of PRIME MAC.

Main features:

- A Service Node can only exchange data with the Base Node and not to other Service Nodes. This meets all the requirements of IEC 61334-4-32, which has similar restrictions.
- Each 4-32 SSCS session establishes a dedicated PRIME MAC connection for exchanging unicast data with the Base Node.
- The Service Node SSCS session is responsible for initiating this connection to the Base Node. The Base Node SSCS cannot initiate a connection to a Service Node. However, once the SSCS session has been established, the Base Node



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**53/83

will always initiate all data transfers with the Service Nodes SSCS session. This meets all the requirements of IEC 61334-4-32.

- Each 4-32 SSCS listens to a PRIME broadcast MAC connection dedicated to the transfer of 4-32 broadcast data from the Base Node to the Service Nodes. This broadcast connection is used when the 4-32 application on the Base Node makes a transmission request with the destination address used for broadcast or the broadcast SAP functions are used. When there are multiple SSCS sessions within a service node, one PRIME broadcast MAC connection is shared by all the SSCS sessions.

See [9] and [8] for further details on addressing issues and the establishment of data sessions.

*7.3.3.1.1 Convergence layer services: opening and closing the Convergence Layer at the Service Node*

- CL432 ESTABLISH: passed from the application to the 4-32 Convergence Layer. It is used to open a CL session and initiate the process of registering the device Serial Number with the Base Node, while this node allocates a destination address to the Service Node session.
- CL432 RELEASE: passed from the application to the 4-32 Convergence Layer. It is used to close the CL and release any resources it might be holding.

*7.3.3.1.2 Convergence layer services: opening and closing the Convergence Layer at the Base Node*

There are no Service Access Point primitives defined at the Base Node for opening or closing the CL.

*7.3.3.1.3 Convergence layer services: Base Node indications*

- CL432 JOIN: to indicate that a Service Node has joined the PRIME subnetwork managed by this Base Node.
- CL432 LEAVE: to indicate that a Service Node has left the PRIME subnetwork managed by this Base Node.

*7.3.3.1.4 Convergence layer services: Data Transfer primitives*

The same data transfer primitives defined in in [9] (§2) are used in this CL.

**7.3.3.2 The IPv4 Convergence Layer**

The IPv4 convergence sublayer (SSCS) provides an efficient method for transferring IPv4 packets over the PRIME network. Its main features are:

- A Service Node can pass IPv4 packets to the Base Node or to other Service Nodes.
- It is assumed that the Base Node acts as a router between the PRIME subnet and the backbone network. The Base Node could also perform NAT.
- In order to keep the implementation simple, only one single route is supported per local IPv4 address.
- The Service Nodes may use statically configured IPv4 addresses or DHCP to obtain IPv4 addresses.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**54/83

- The Base Node performs IPv4 to EUI-48 MAC address resolution. Each Service Node registers its IPv4 address and EUI-48 MAC address with the Base Node. Other Service Nodes can then query the Base Node to resolve an IPv4 address into a EUI-48 MAC address. This requires the establishment of a dedicated connection to the Base Node for address resolution.
- The convergence layer performs the routing of IPv4 packets. In other words, the convergence layer will decide whether the packet should be sent directly to another Service Node or forwarded to the configured gateway.
- Although IPv4 is a connectionless protocol, the IPv4 convergence layer is connection-oriented. Once address resolution has been performed, a connection is established between the source and destination Service Node for the transfer of IP packets. This connection is maintained while traffic is being transferred and may be removed after a period of inactivity.
- Optionally TCP/IPv4 headers may be compressed. Compression is negotiated as part of the connection establishment phase.
- The Broadcasting of IPv4 packets is supported using the MAC broadcast mechanism.
- The multicasting of IPv4 packets is supported using the MAC multicast mechanism.
- Segmentation and reassembly services are provided by the CPCS.

The convergence layer has a number of connection types. For address resolution there is a connection to the Base Node. For IPv4 data transfer there is one connection per destination node: the Base Node that acts as the IPv4 gateway to the outside world or to another node in the same subnetwork.

*7.3.3.2.1 Services: opening and closing the Convergence Layer*

- CL IPV4 ESTABLISH: passed from the IPv4 layer to the IPv4 convergence layer. It is used when the IPv4 layer brings the interface up.
- CL IPV4 RELEASE: passed from the IPv4 layer to the IPv4 convergence layer. It is used when the interface is put down.

*7.3.3.2.2 Services: unicast address management*

- CL IPV4 REGISTER: passed from the IPv4 layer to the IPv4 convergence layer. It is used to register an IPv4 address.
- CL IPV4 UNREGISTER: passed from the IPv4 layer to the IPv4 convergence layer. It is used to unregister an IPv4 address.

*7.3.3.2.3 Services: multicast group management*

- CL IPV4 JOIN: passed from the IPv4 layer to the IPv4 convergence layer. It contains an IPv4 multicast address that is to be joined.
- CL IPV4 LEAVE: passed from the IPv4 layer to the IPv4 convergence layer. It contains an IPv4 multicast address that is to be left.

*7.3.3.2.4 Services: data transfer*

- CL IPV4 DATA: passed from the IPv4 layer to the IPv4 convergence layer. It contains one IPv4 packet to be sent, or indicates the arrival of one IPv4 packet.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**55/83

### 7.3.4 Networking Layers (Network, Transport)

The standard IP network layer (see [20] for further details) and TCP/UDP transport layer are used for the IP-based profile over PRIME to transport DLMS/COSEM APDUs.

[21] defines a TCP/IP wrapper for DLMS/COSEM when using the IP-based profile. A wrapper layer is specified which is located between the COSEM Application layer and the TCP layer.

Its role is to transform OSI style service requests/responses to and from TCP function calls. In addition, it provides addressing for the logical devices and length information about the payload to be transported. The latter is necessary as the TCP layer (see [36]) will transport its payload in segments of various lengths, and therefore the receiving end will be able to detect the end of the message only if its length is known.

The port number assigned for DLMS/COSEM by the IANA is 4059.

The COSEM UDP-based transport layer includes the Internet standard UDP layer, as specified in [22], and the COSEM-specific lightweight wrapper sublayer. In this communication profile, the wrapper sublayer is a state-less entity: its only roles are to ensure source and destination COSEM AP identification using the wPort numbers and to provide conversion between the OSI-style UDP-DATA.xxx service invocations and the SEND() and RECEIVE() interface functions provided by the standard UDP. Although it is not necessary in the UDP-based profile, in order to have the same wrapper protocol control information (i.e. the wrapper header) in both COSEM transport layers, the wrapper sublayer shall also include the Data Length information in the wrapper protocol data unit.

No network neither transport layers are used for a 4-32 based profile over PRIME.

### 7.3.5 Upper layers (Session, Presentation, Application)

See 7.2.4.

### 7.3.6 Data Model

See 7.2.5.

### 7.3.7 Security

Apart from information in 7.2.6 which is still valid, there are security mechanisms that can be applied independently, or in conjunction with DLMS/COSEM security mechanisms. For PRIME, the security functionality provides the MAC layer with privacy, authentication and data integrity through a secure connection method and a key management policy. All packets must use the negotiated security profile. The only exceptions to this rule are the REG and SEC control messages, and the Beacon PDU and Promotion Need PDUs which are transferred non-encrypted.

Several security profiles are provided for managing different security needs, which can arise in different network environments. Up to now, the current version of the PRIME specification lists two security profiles and leaves scope for adding up to two new security profiles in future versions.

Communications having Security Profile 0 are based on the transmission of MAC SDUs without encryption. This profile shall be used by communication that does not have strict requirements on privacy, authentication or data integrity.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**56/83

Security Profile 1 is based on 128-bit AES encryption of data and its associated CRC. This profile is specified with the aim of fulfilling all security requirements:

- Privacy is guaranteed by the encryption itself and by the fact that the encryption key is kept secret.
- Authentication is guaranteed by the fact that each node has its own secret key known only by the node itself and the Base Node.
- Data integrity is guaranteed by the fact that the payload CRC is encrypted.

The cryptographic algorithm used in this specification is the AES, as specified in [6]. The standard describes the algorithm with three possible key sizes; the 128-bit secret key represents a good level of security for preserving privacy up to 2030 and beyond, as recommended by [24].

AES is used according to the so-called Electronic Code Book (ECB). It is a block-ciphering mode where plain text is divided into 128-bit blocks. Padding is applied if the last block is smaller than 128 bits. Padding is implemented with the addition of a bit equal to 1 and as many zeroes as necessary to reach a length of the string to be encrypted as a multiple of 128 bits. Encryption is performed one block at a time, using the same working key for all the data.

See [8] for additional references and further information.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**57/83

## **8 MI2-SI2 (Electricity Meter/Communication hub-Central System)**

### **8.1 Introduction**

MI2-SI2 is the interface directly linking the Electricity Meter/Communication Hub with the Central System. Due to cost constraints, this will be usually cellular. If a large number of nodes are installed using the network of a telecom provider operation costs may become significant. In this case data exchange with the meter has to be kept at a minimum.

A large number of nodes to be managed by the Central System imply this interface does not usually have high bandwidths from the electricity meter perspective.

GPRS/UMTS wireless technology was considered by [2] to be most suitable technology for this interface. A Protocol Architecture will be studied for DLMS/COSEM.

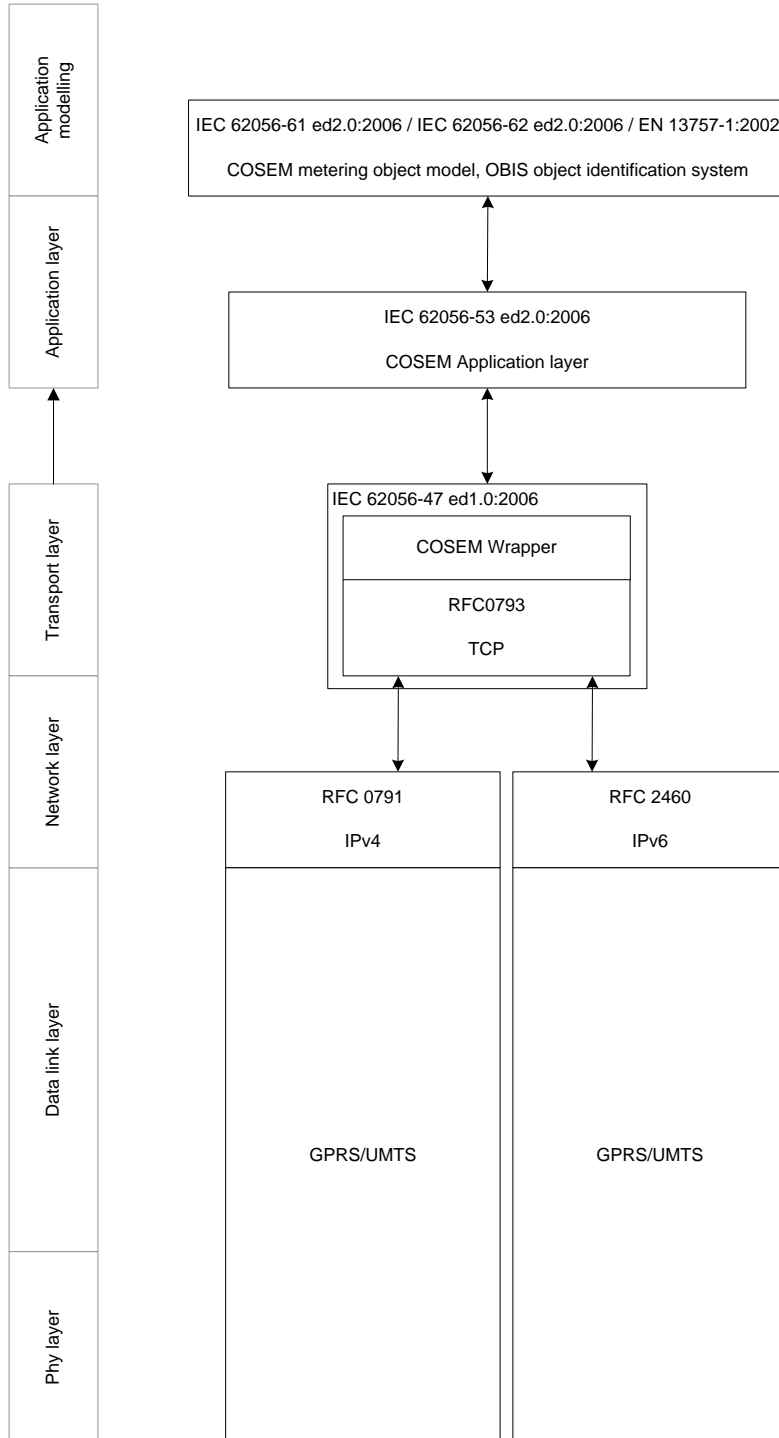


Figure 10 - MI2-SI2 interface communications architecture

## 8.2 Subnetwork Layers



**Energy Theme; Grant Agreement No 226369**

**8.2.1 GPRS (2.5G)**

GPRS (General Packet Radio Service) is a mobile data service offered in GSM systems, in addition to GSM service (it is integrated into GSM Release 97 and newer releases). It was originally standardized by European Telecommunications Standards Institute (ETSI) and now by the 3<sup>rd</sup> Generation Partnership Project (3GPP). It is nowadays globally available in nearly all countries (except e.g. South Korea and Japan). In general terms, GPRS coverage is readily available in populated areas in most countries. The technology is stable, as analyzed in [23].

GPRS is widely used in IP networks today as a WAN wireless (cellular) technology. Each GPRS subscriber obtains an IP address, which can be public or private, and at the same time fixed or dynamic, depending on the contracted service features and operator capabilities.

GPRS service is provided in the GSM licensed frequency bands of 800 MHz, 900 MHz, 1800 MHz and 1900 MHz.

The GPRS Access network is divided into two sections:

- GERAN (for GSM Radio Access Network) which comprises all the layers 1, 2 and 3 for the radio access network, plus all the normalized interfaces between them.
- The GSM core network, comprising the GSM network switching subsystem, the Gateway GSM support nodes (GGSN) and the Service GSM support nodes (SGSN).

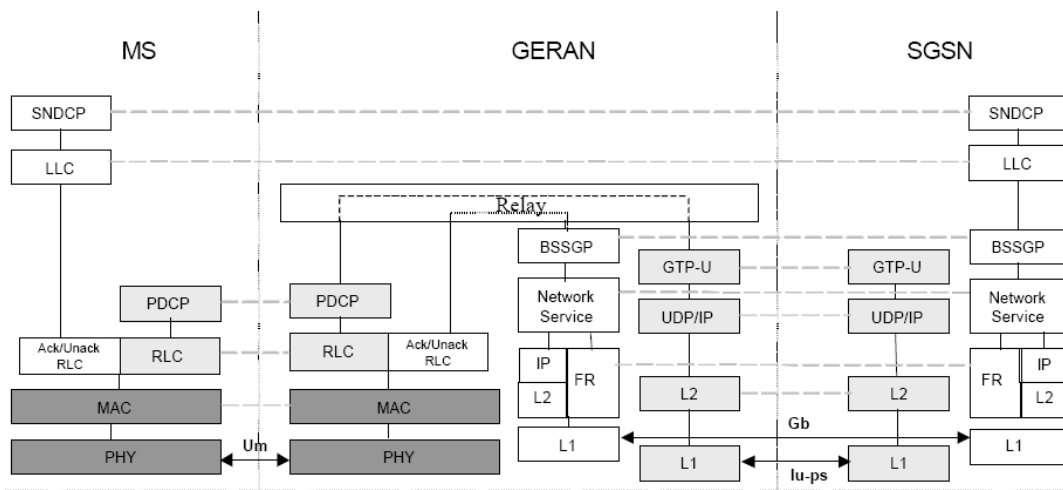


Figure 11 - Protocol overview of the GPRS network.

An electricity meter would function as an MS (Mobile Station) from a GPRS perspective.

**8.2.2 UMTS (3G)**

UMTS (Universal Mobile Telecommunications System), also known as 3G or third generation mobile technology, is an evolution of existing 2G/GPRS networks using WCDMA modulation techniques in the air interface. It is specified by 3GPP and is part



**Energy Theme; Grant Agreement No 226369**

of the global ITU IMT-2000 standard. There have been different releases of UMTS issued by 3GPP.

The UMTS lower layer networks are owned by the mobile operator. This network can be further subdivided into two different sections:

- UTRAN (UMTS Terrestrial Radio Access Network), which contains the nodes B (Base Stations) and RNCs, which comprise the Radio Access Network. This network provides the coverage area, linking the Electricity Meter/Communication hub with the UMTS core network. Each of the different network sections in UTRAN contains standard interfaces to the others, so the technology can be easily upgraded while maintaining full compatibility. All of this is specified in the 25 series of 3GPP specifications (i.e. documents TS25.xyz).
- The Core Network, linking all the RNCs. The UMTS core network is an evolution of the previous 2G (GSM) core networks. It is an access-agnostic network, where some services can be directly connected to the core network.

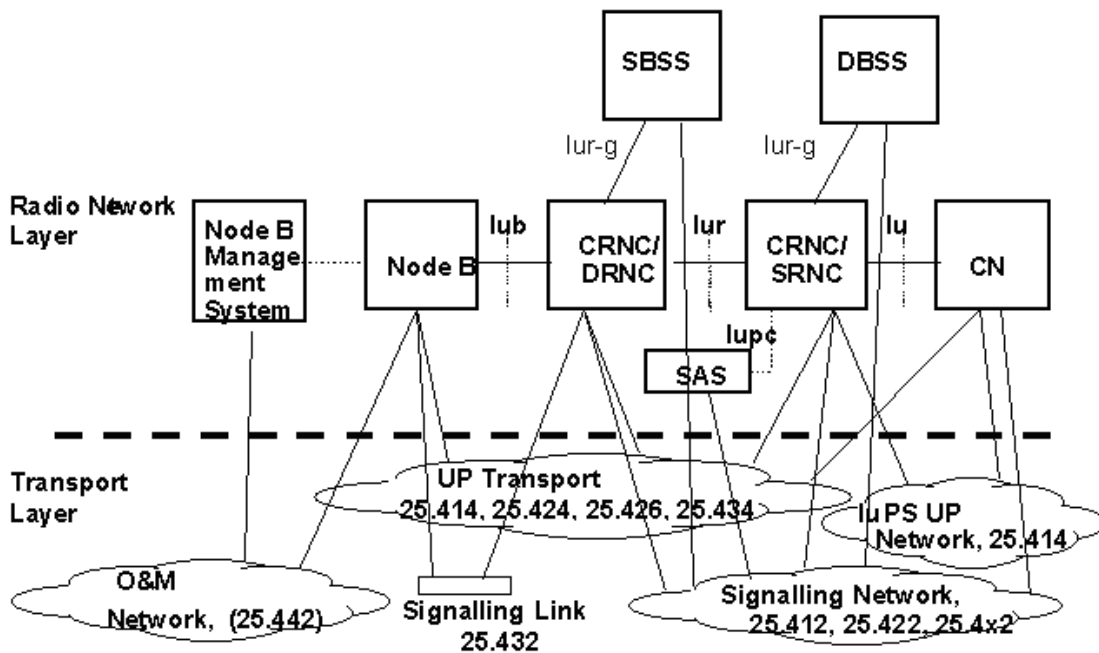


Figure 12 - UTRAN protocol layering, interfaces and specification references

## 8.3 Networking Layers

### 8.3.1 Network layer: IPv4/IPv6

IPv4 (see [20]) and IPv6 (see [25]) protocols have been taken into account for the architecture design. IPv4 is used over GPRS/UMTS nowadays so no new implementation or researches are needed.

The fact is that IPv6 provides better performance and solves the problem of IP addressing that will soon appear with IPv4, so IPv6 must also be supported. There are IPv6 standards documents such as [25] but more specification is necessary for the optimal use of IPv6 in a cellular environment. The characteristics of cellular links in



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**61/83

terms of cost, bandwidth and delay put special requirements on how IPv6 is used. [26] proposed by Ericsson and Nokia considers IPv6 for cellular hosts that attach to GPRS/UMTS networks.

Operators in Europe are still reluctant to make the changes needed at their networks to support IPv6, but some projects in Europe (e.g. 6WINIT *IPv6 Wireless Internet Initiative* where Ericsson took part) show that technically IPv6 over wireless GPRS/UMTS networks is possible.

It is necessary to investigate how IPv6 over wireless GPRS/UMTS protocols is being implemented.

### **8.3.2 Transport layer**

International standard [21] specifies the transport layer architecture for DLMS/COSEM over IPv4 layers. This standard specifies a connection-oriented transport layer, based on TCP, which will be used for OPEN meter MI2-SI2 interface. It also adds a sublayer called “wrapper”, by which the information coming from the upper application layer is encapsulated and the requests and responses processes accordingly, in order to deliver it to the TCP transport sublayer, depending on the type of DLMS/COSEM service. It is thus a conversion between DLMS application layer interface and TCP transport layer interface. See 7.3.4 for further information.

## **8.4 Application Layers**

DLMS Application layer is described in [11], developed and maintained by the DLMS User Association. It specifies services to access the attributes and methods of COSEM objects. See 7.2.4.

## **8.5 Data Model**

The data model is independent of the communication profile. For details see 7.2.5.

## **8.6 Security**

GPRS/UMTS wireless technology is IP based, so all standard security protocols on the TCP/IP stack such as IPSec, TLS/SSL, etc. can be implemented over GPRS/UMTS, in order to have secure communication links.

On the other hand, security can also be addressed at the application layer. For a detailed discussion on the security features of DLMS/COSEM see 6.2.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**62/83

## **9 MI3 (Electricity Meter/Communication hub-Local O&M device)**

### **9.1 Introduction**

The MI3 interface is used by HHUs or portable devices to interact with electricity meters during the installation process or maintenance. The interface MI3 can also be used for communication with the meter, if the remote connection via interface MI1 or MI2 is temporarily unavailable.

### **9.2 DLMS/COSEM over optical interface**

The proposed local interface of the electricity meter is based on the DLMS/COSEM serial, three-layer profile over an optical port. This comprises the COSEM application layer, the HDLC-based data link layer and the physical layer for connection-oriented asynchronous data exchange.



**Energy Theme; Grant Agreement No 226369**

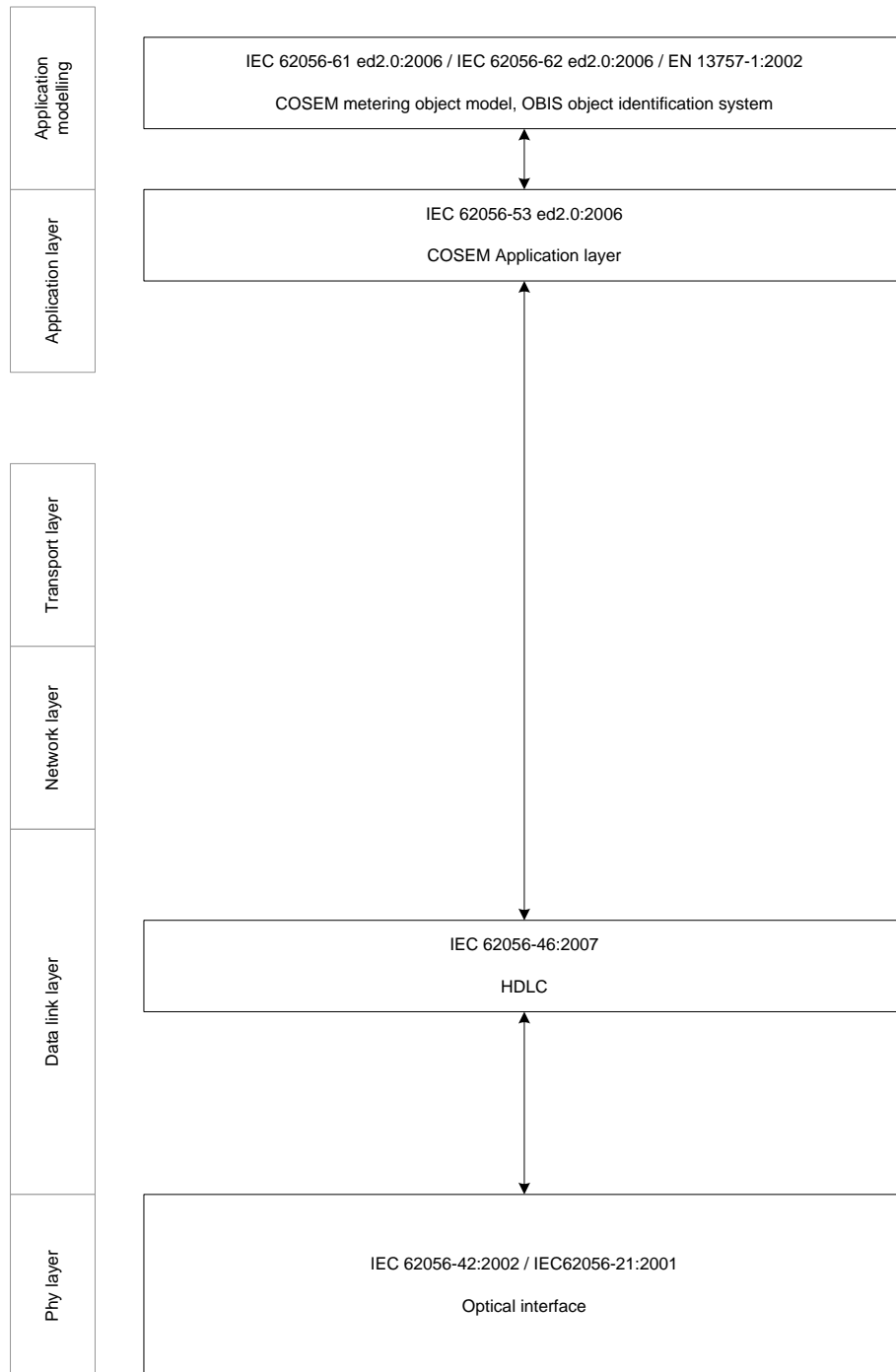


Figure 13 - MI3 interface communications architecture

### 9.2.1 Physical Layer

The serial, optical interface as described in [27] is used. The necessary services are defined in [28].

### 9.2.2 Data Link Layer

The data link layer uses the HDLC protocol as defined in [29].



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture      **Version:** 1.1      **Page:**64/83

In fact it is split in an LLC sublayer and the HDLC protocol layer:

- The LLC sublayer based on [10]. Here, it is used in an extended Class I operation. The only role of this sublayer is to select the COSEM Application layer by using a specific LLC address. The LLC services are provided by the HDLC based MAC sublayer;
- The MAC sublayer, based on the HDLC protocol. It provides addressing of application entities within the equipment.

The HDLC based LLC sublayer provides the following services:

- DL-Connect services to connect and to disconnect the data link layer;
- Connection oriented DL-Data services for transporting ACSE APDUs and xDLMS APDUs. These services provide reliable data transport and support segmentation to carry long messages, in a transparent manner for the application layer.

### **9.2.3 Application Layer**

The application layer is the COSEM Application layer as specified in [11]. It provides services to the COSEM application process (AP) and uses the services of the HDLC based LLC sub-layer. See 7.2.4.

### **9.2.4 Data Model**

The data model is independent of the communication profile. For details see 7.2.5.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**65/83

## 10 MUMI2 (Multi-utility meter-Local O&M device)

### 10.1 Introduction

The interface to local Operations and Maintenance devices for battery-operated, low-cost, multi-utility meters has to meet important constraints with respect to complexity and price.

Although the proposal in [3] is to use already existing wireless standards such as WiFi or IEEE 802.15.4 for this communications interface, it is believed that these technologies will be too complex to adapt to MUMI2 ports while meeting stringent complexity limits for the multi-utility meters. Certainly the gap to be bridged inside WP3 is considered too big for the resources in the Project. Additionally, defining new, open PHY and MAC layers from scratch for such an interface is considered out of OPEN meter scope.

Taking into account that no proprietary solutions would be accepted inside OPEN meter, the proposal for this interface is to actually integrate O&M functions into MUMI1 interface, so the local configuration and maintenance of a multi-utility meter will be done via MUMI1-MI4 interface. The access to the MUMI1 port can then be performed via a local device which acts as a COSEM client or either remotely, via the Electricity Meter/Communication hub.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**66/83

# 11 MUMI1-MI4 (Multi-utility meter - Electricity Meter/Communication hub)

## 11.1 Introduction

The following profiles for the multi-utility meter communications interface MUMI1-MI4 are proposed:

Table 7 - MUMI1-MI4 interface communication architecture choices

Short name	Phy medium	Phy layer	Link layer	Application layer
M-bus TP	Twisted pair base band signalling	EN 13757-2	EN 13757-2	M-Bus dedicated application layer EN 13757-3 + IEC 62056-53 DLMS/COSEM
M-Bus TP DLMS/COSEM	Twisted pair	EN 13757-2	IEC 62056-46 HDLC	IEC 62056-53 DLMS/COSEM
Wireless M-Bus	Radio 886 MHz	EN 13757-4 various modes	EN 13757-4	M-Bus dedicated application layer EN 13757-3 + IEC 62056-53 DLMS/COSEM
Euridis 2 DLMS/COSEM	Twisted pair carrier signalling	IEC 62056-31 Ed.2: 200x	IEC 62056-31 Ed.2: 200x	IEC 62056-53 DLMS/COSEM
IEEE 802.15.4 radio	Radio 886 MHz or 2,4 GHz	IEEE 802.15.4	IEEE 802.15.4	IEC 62056-53 DLMS/COSEM
ZigBee DLMS/COSEM tunneling	Radio 886 MHz or 2,4 GHz	IEEE 802.15.4	IEEE 802.15.4	IEC 62056-53 DLMS/COSEM

The twisted pair profiles are proposed additionally to suggestions of [3], because of the following advantages for multi-utility meters:

- Twisted Pair bus can provide power;
- “Paired” installations of electricity and e.g. natural gas in close proximity are not uncommon in many countries;
- Hardwired pairing of multi-utility meter and communication hub, therefore no special pairing procedures are needed - no data security and integrity issues.

In [3] there is a suggestion for the use of IEEE 802.11 (WiFi); this is not considered here and the proposal is to remove such suggestion in future revisions of WP2 deliverables. The main reason for this is the fundamental requirement of “low-power” for multi-utility meters, which is deemed impossible to fulfill with the current IEEE 802.11. The necessary step improvement in term of power consumption is too large and beyond what can be covered in OPEN meter scope.



**Energy Theme; Grant Agreement No 226369**

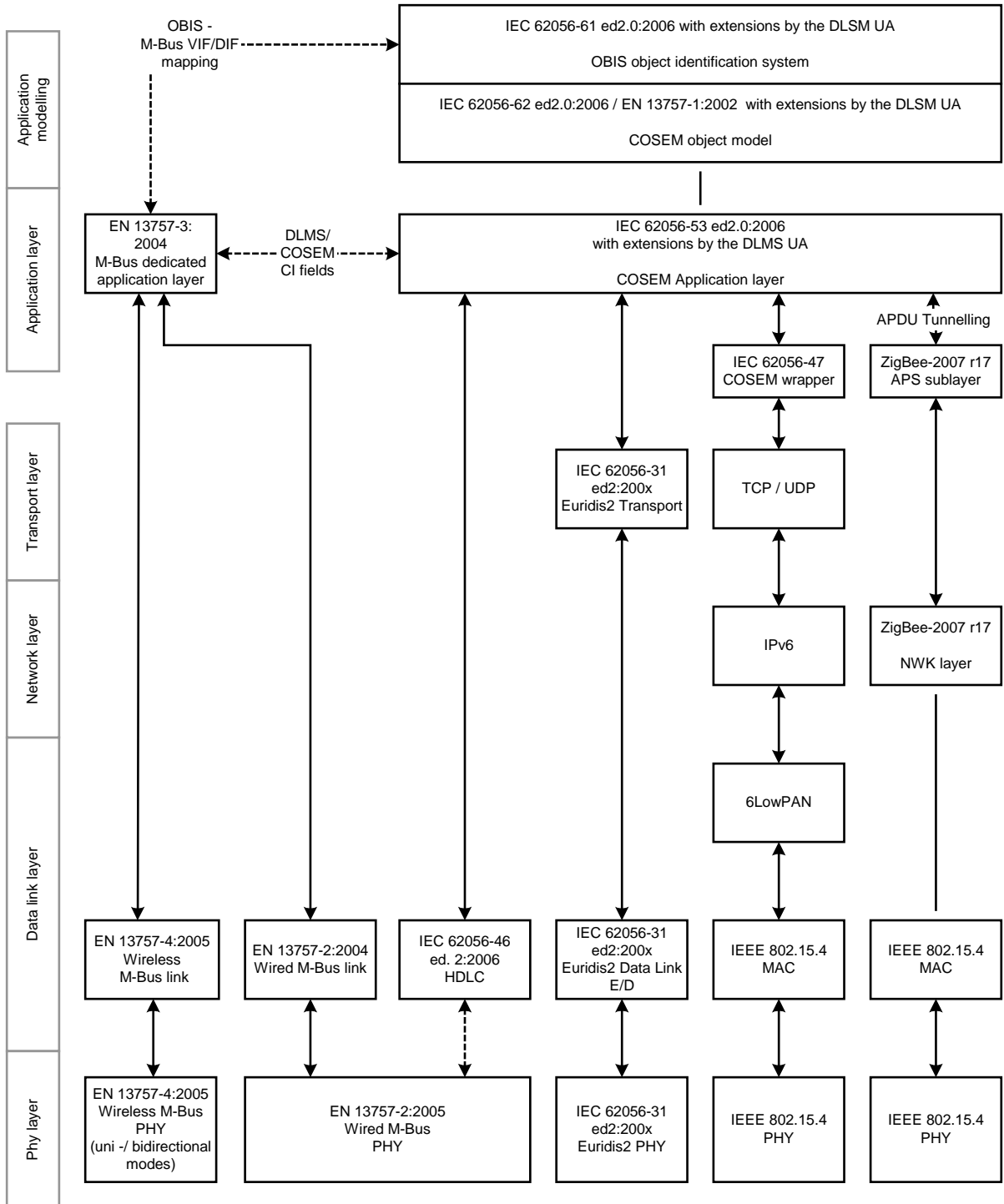


Figure 14 - MUMI1-MI4 interface profiles

## 11.2 M-Bus twisted pair

*NOTE This profile is closely following the Open Metering System Specification (OMS – Issue 1.2.0, 2009).*



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**68/83

### 11.2.1 Physical layer

For wired connections the physical layer M-Bus according to the European standard [30] is proposed. It is a two-wire system, optionally capable of providing power to multi-utility (battery-powered) meters.

The bus interfaces of the slaves are polarity independent, which means the two bus lines can be interchanged without affecting the operation of the slaves. Besides protection aspects, this also results in a simplified installation of the bus system. In order to maintain correct operation of the bus in case of a short circuit of one of the slaves, these must have a protection resistor with a nominal value of  $430 \pm 10 \Omega$  in their bus lines. This limits the current in case of a short circuit to a maximum of 100mA ( $42 \text{ V}/420 \Omega$ ), and reduces the energy converted into heat in the bus interface. For the requirements for wiring and installation, refer to [30].

### 11.2.2 Data link layer

The link layer is fully described in [30] (§5).

### 11.2.3 Network/transport layer

Since this profile just describes a direct point to point link, no network/transport layer is needed.

### 11.2.4 Application layer

The M-Bus dedicated application layer has always a fixed frame structure as described in [31]. It may transport either the meter application layer according to EN13757-3:2004 (M-Bus dedicated application layer), or alternatively EN13757-1:2002 (DLMS/COSEM-type communication, see [33]).

The choice between the two alternative solutions depends on the properties of the physical medium, the limitations imposed by the power supply (battery or mains) and the set of smart metering use cases to be supported. This has to be further analyzed during the OPEN meter Project.

Note that the CI field as the first byte of the application layer telegram distinguishes between these application layer protocol types and frame structures.

At this time, we are not aware of any implementations using the CI fields for carrying DLMS/COSEM APDUs. Therefore this is identified as a gap which needs further consideration in the OPEN meter Project.

## 11.3 M-Bus twisted pair DLMS/COSEM

This profile uses only the physical layer of M-Bus, carrying HDLC frames transporting DLMS/COSEM APDUs.

The profile proposed here has already been implemented in metering devices, but it is not yet part of the DLMS/COSEM specification and of the IEC 62056 / EN 13757 series.

### 11.3.1 Physical layer

See 11.2.1.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**69/83

### 11.3.2 Data link layer

The data link layer is as specified in [29]. It is based on the HDLC protocol specified in [34]. It provides the following key features:

- Source and destination addressing. Application associations are bound to these addresses;
- Segmentation: long messages can be transported in shorter segments;
- Window sizing: several frames may be sent before an acknowledgement of reception is required.

### 11.3.3 Application layer

The Application layer is the DLMS/COSEM application layer specified in IEC 62056-53 and its extensions by the DLMS UA. See 7.2.4.

This Application layer works with the COSEM objects specified in IEC 62056-62 and IEC 62056-61, with extensions by the DLMS UA.

## 11.4 Wireless M-Bus

*NOTE: This profile is closely following the Open Metering System Specification (OMS – Issue 1.2.0, 2009).*

### 11.4.1 Introduction

Wireless M-Bus has been optimised for low battery consumption and short duty cycles. It provides various modes to support different scenarios like stationary and mobile readout.

The main direction of the traffic is from the meter to the data collector system, with a back channel for commands, especially when the meter is battery powered. In the case of mains powered meters, there are fewer limitations.

To support smart metering uses cases requiring full two-way communication, the main candidates are modes S2 and T2.

In the next stages of the OPEN meter Project, a gap analysis has to be performed to verify which smart metering uses cases can be supported using wireless M-Bus.

### 11.4.2 Physical layer

[32] describes several variants for wireless meter communications. They cover all types of meter communication including mobile and stationary readout modes. A smart meter scenario requires a stationary receiver and frequent transmission of meter data to support user consumption feedback and variable tariffs.

There are various modes described in [32]. All these modes operate in various duty-cycle limited sub-bands of the 868-870MHz license-free frequency range. The duty cycle limits the band occupation time from other systems operating in these frequency bands.

S1 and T1 are unidirectional standards where the meter frequently (seconds to hours) transmits telegrams containing meter identification together with metered data.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**70/83

S2 and T2 are compatible bidirectional enhancements of S1 respectively T1. Both enable a communication hub to multi-utility meter communication after each multi-utility meter to communication hub telegram.

### 11.4.3 Data link layer

The data link layer is fully described in [32].

#### 11.4.1 Network/transport layer

If a direct wireless transmission between a multi-utility meter and a communication hub is not possible a single intermediate repeater might be used. Such a repeater shall be able to work without complex installation procedures and without routing capability. For a common device management a repeater shall send telegrams with its own address to provide device management data like status. A repeater conforms to general rules like every multi utility meter.

A repeater may be a dedicated device or a function integrated into a multi-utility meter or a communication hub.

#### 11.4.2 Application layer

See 11.2.4

## 11.5 Euridis2 DLMS/COSEM

Architecture using the COSEM application layer adopts a 4 layer protocol: Physical, Data Link, Transport and Application, with an extra layer, enabling communication management support.

In this architecture, the physical and data link layers are the same as those used in the DLMS model, with 2 differences:

- The management of speed negotiation;
- All services related to communication support management are now moved from the data link layer to a new layer entitled the support manager layer.

The data link layer interfaces at the upper level to two specific layers:

- A transport layer IEC 62056-31 which enables the fragmentation and reassembly of the Application data units, during data exchange;
- A support manager layer, which has the role of managing all processes specific to the management of the Euridis bus, in order to liberate the data link and application layers. (This support manager layer is not shown in Figure 14.)

Above the Transport layer, The COSEM Application layer is used (see 7.2.4). This architecture enables the use of COSEM object modelling and of object accessibility services managed by it on the Euridis bus.

The proposed Euridis2, protocol specified in [35] is an extension to the original Euridis protocol, allowing fully compatible and non-interfering transport of DLMS/COSEM application objects on a Euridis infrastructure.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**71/83

### 11.5.1 Physical layer

The physical layer is described in [35]. It uses an amplitude modulated 50 kHz carrier on a twisted pair link. Data transmission is half-duplex at a rate of 1200 bit/s. The new version of Euridis supports speed negotiation up to 9,600 baud.

Optionally, the bus can transport a DC voltage for energy supply of multi-utility meters.

### 11.5.2 Data link layer

The data link layer is fully described in [35].

### 11.5.3 Transport layer

The role of the transport layer is to ensure the fragmentation and reassembly of the application data units. It is fully specified in [35].

### 11.5.4 Support manager layer

The Support Manager layer processes all services related to communication support. These services are:

- Initialization of the bus;
- Discovery management;
- Alarm management;
- Speed negotiation.

### 11.5.5 Application layer

The IEC 62056-53 COSEM application layer is used.

## 11.6 IEEE 802.15.4 radio

This profile is the same as the one used for MI5. It uses 6LoWPAN described in RFC4944.

## 11.7 ZigBee

This profile will be based on IEEE 802.15.4 radio, tunneling COSEM APDUs for complex meter data through the ZigBee Smart Energy Profile.



**Energy Theme; Grant Agreement No 226369**

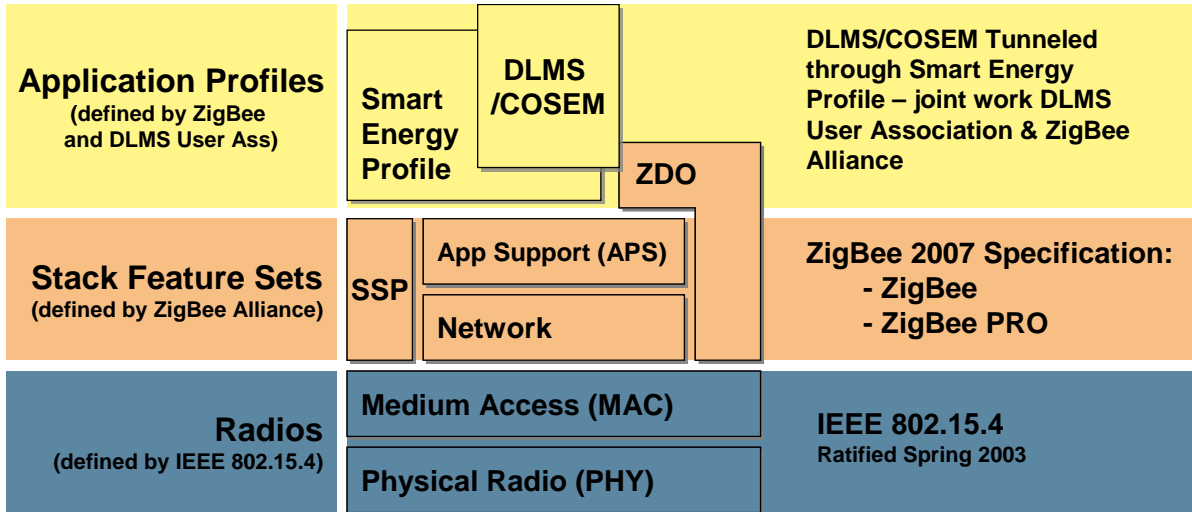


Figure 15 - ZigBee stack architecture

**11.7.1 Physical layer**

The physical layer uses low power radio, defined by IEEE 802.15.4-2006. Frequency options are 2.4 GHz (preferred) and 868 MHz.

**11.7.2 Data link layer**

The data link layer is specified in IEEE 802.15.4-2006.

**11.7.3 Network/transport layer**

ZigBee PRO Stack includes Network organisation, route discovery, device discovery, message relay & security. It provides mesh network implementations primarily for in-home networks.

**11.7.4 Application layer**

The ZigBee Application Sublayer (APS) defined in the ZigBee Specification 2007 shall interface to the COSEM Application layer (IEC62056-53) for complex metering data objects and with the ZigBee Smart Energy Profile Application layer for simple meter data objects.

The Smart Energy Profile is used where DLMS/COSEM is not established for in home device interoperability (e.g. meters, displays and other demand side management devices to and from the communications hub). The Smart Energy profile also supports manufacturer specific data transfers.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**73/83

## **12 MI5 (Electricity Meter/Communication hub-End Customer devices)**

### **12.1 Introduction**

MI5 interfaces the Electricity Meter/Communication hub with the End Customer devices (e.g. in-home display, Energy-box, energy management devices, etc.). In [3] both ZigBee and Bluetooth are considered to be the most suitable technologies.

In order to build complete communication profiles proposal for this interface, DLMS and ZigBee Smart Energy Profile application layers have been integrated.

### **12.2 Communication profiles proposal**

Based on the technologies selected by WP2, different complete communication profiles are proposed below. They have been chosen according to the combinations that are commonly used at the moment.

Nevertheless, when it comes to the Home Automation world, things are evolving very quickly, and both the architectures and the technologies that will be used during the lifespan of the smart meters currently being defined are uncertain.

In any case for low bandwidth radio, the standard IEEE 802.15.4 is already a reality. It is the base of two different communication stacks 6LowPan and ZigBee, which have in common many characteristics. These two stacks might merge into one single communication profile sooner or later.

As far as Bluetooth technology is concerned in its current state, its future for Home Automation purposes does not seem to be so clear. Originally Bluetooth was conceived for handheld devices, and its rather high consumption and short range coverage make this technology less suitable for Home Automation purposes.



**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**74/83

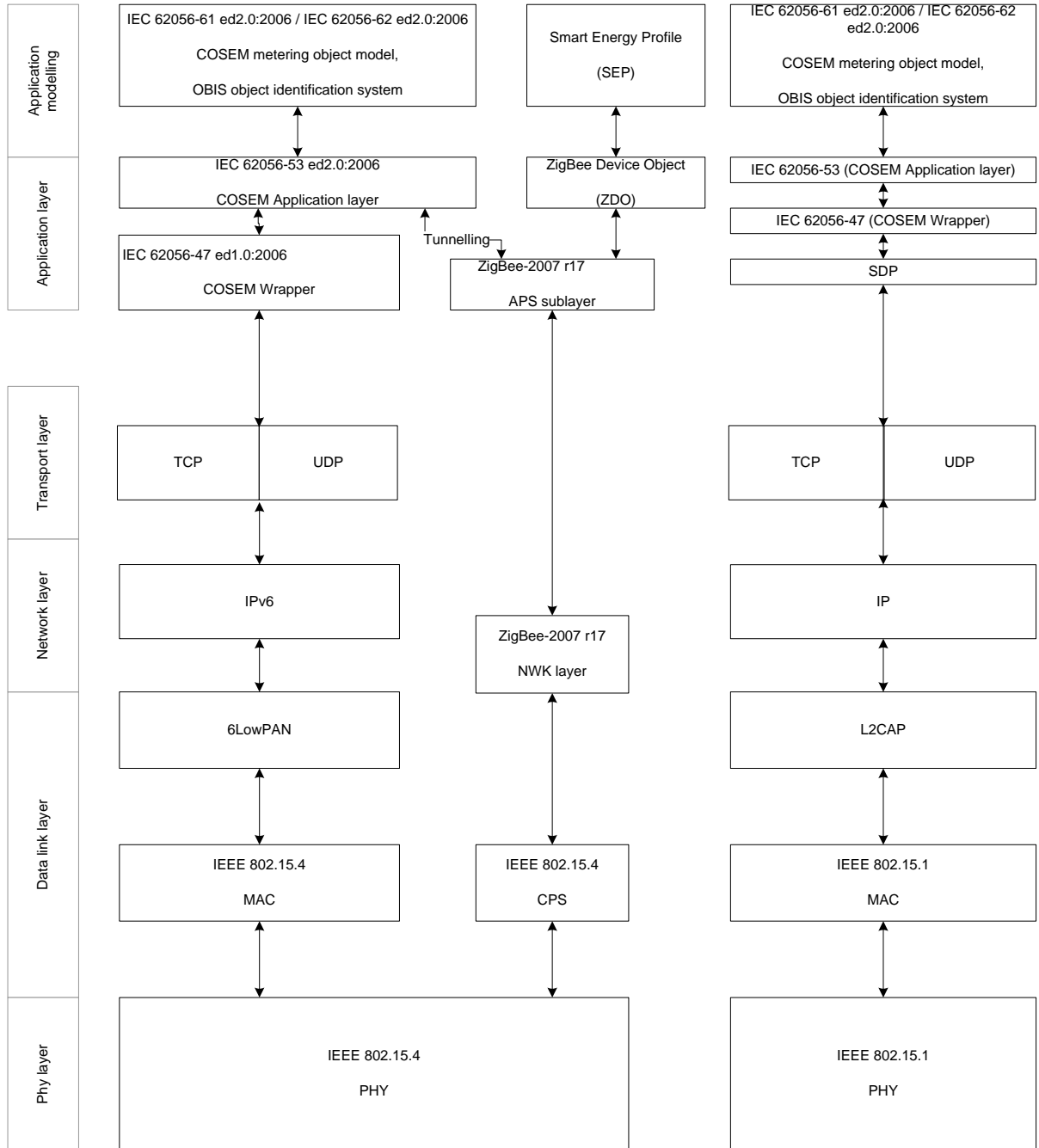


Figure 16 - MI5 interface profiles



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**75/83

## 13 CI2-SI1 (Concentrator-Central System)

### 13.1 Introduction

Two protocol profiles are proposed: A new highly scalable solution based on SNMPv3 plus Secure file transfer protocol (sftp) and a Web Services-based profile.

First, the common lower layers of the protocol profiles are briefly described, and then those two different protocol profiles are introduced.

Next, both protocol profiles are either discussed in detail or a reference is made to the already existing standards.

*NOTE: Since the CI2-SI1 interface is based on wide area network technologies, a full suite of standards, built around the IP protocol, is available for lower layers of the CI2-SI1 interface communication profile. On the contrary, the upper layers of this communication profile, which are strongly linked to the metering requirements and utility's inner organization, are still under consideration. Notwithstanding the fact that some orientations concerning the upper layers will be described in this chapter based on Web Services, the gap regarding the application layer and the application modeling has been identified, and it will be developed in WP3. For the time being, the presented application layer and application modeling have to be considered just as a possible orientation.*

### 13.2 Physical Layers

The profiles do not make any assumption about the physical layer.

### 13.3 Network and Transport Layers

[3] included GPRS and UMTS as candidate transport technologies for the interface CI2-SI1 between Concentrator and Central System. However, any technology providing IP as the network layer with sufficient bandwidth and latency is suitable, e.g. broadband over power line.

### 13.4 Protocol Profiles

There are two proposed set of protocols, henceforth called profiles, for the interface CI2-SI1. One profile is based on SNMPv3 plus SSH-2 sftp, the other profile is the based on Web Services and reflects the Dutch smart metering recommendation.



**Energy Theme; Grant Agreement No 226369**

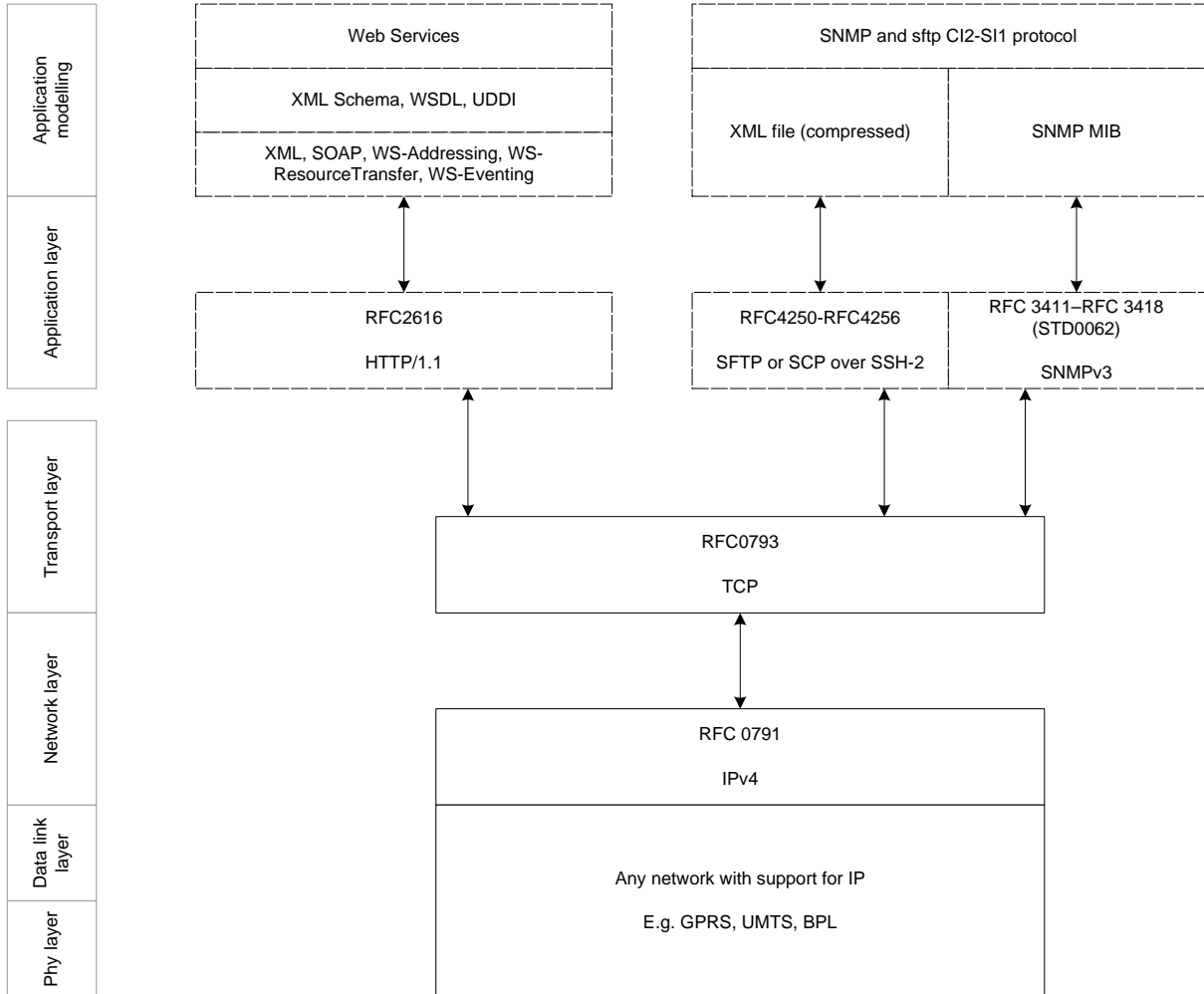


Figure 17 - The two profiles for CI2-SI1

**13.4.1 Profile 1 - SNMPv3 and sftp**

**13.4.1.1 Architecture of the SNMP and sftp profile**

This proposed CI2-SI1 protocol profile uses a combination of two standard protocols: SNMPv3 and sftp protocol.

SNMP is a standard protocol widely used in network management. It has advantages of simplicity of implementation, excellent support and an extensible, compliable management information base (MIB) that provides mechanisms for standards definitions and vendor extensions. SNMPv3 adds encryption, authentication and authorization using MIB views to the standard SNMP capabilities.

The MIB views can be used to separate the network management functions from the meter data collection functions. Utilities can use MIB views to segment functional access without compromising role-based security models.

Secure file transfer protocol (sftp) is proposed to address the large amount of data transferred by the Concentrator. Data files are compressed prior to sftp transfers. All



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**77/83

up/downloads are coordinated by the Central System with SNMPv3 commands. The Concentrator will send notification over SNMP that new data is available.

Furthermore, usage of the SNMP and sftp protocols has the following advantages:

- Relatively simple protocol stack (as compared to e.g. Web Services) with built in security;
- Using SNMP as the protocol for managing the Concentrator allows unifying communication security (SNMPv3 authentication) and management data encryption (all of the SNMPv3 communications are encrypted) for many modules/services that a Concentrator unit can provide:
  - Network Management (setting up IP addressing/routing/ etc.);
  - MI1-CI1 management and diagnostics of the Concentrator (via the MI1-CI1 MIB);
  - Management of the Collector functions (setting up meter services and commanding meters).
- Authentication and security is standard and relatively simpler with SNMP (than e.g. with Web Services). The SNMP stack does not require implementation of HTTP, SOAP protocols, HTTPS and SSL - it was designed for remote management of equipment and the specification unifies all of the functions needed for these operations. Key management and rotation of security keys is built in into the specification - also if any other protocol is required for data transfer (sftp) SNMP provides a secure channel to send down SSH keys passwords or security credential for other protocols.
- Good asynchronous notification model that is designed to be lightweight to allow back-office systems to process massive numbers of informs very quickly;
- Robust way to send asynchronous notifications to multiple listeners (this is harder to achieve with Web Services). Also SNMP has less overhead for data transfers (less bandwidth is required).
- With sftp data transfers data can be compacted in a less verbose way than XML, compressed before it is sent. Also results from multiple services can be batch transferred in a single transaction giving more control to the Central System to control system load, and optimize if needed.
- The SNMP protocol allows a very simple implementation of the pull model, while e.g. the Web Services notifications and operations are lot more synchronous so they would look more like the push model.

### **13.4.2 Profile 2: Web Services-based profile**

#### **13.4.2.1 Overview**

An alternative for the interface CI2-SI1 is based on XML/Web Services. It defines a communications interface for CI2-SI1 that is based on the Web Services architecture according to the extended WS-I Basic Profile 1.2 that supports Resource based Publish/Subscribe Message Exchange Pattern (MEP). The goal is to define an open, standardized protocol implementation based on XML/Web Services.

The usage of Web Services brings the following advantages:



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**78/83

- Web services have better tools to define data schema. This profile specifies a generic structure of the protocol resources that can be expanded to include specific services with parameter and data response definitions. An XSD schema for such final service would describe all of the data specific response fields. A MIB definition will stay in the generic form, without implicitly providing documentation on how COSEM data responses for COSEM commands would look like.
- Web services operate on Object level - providing a concept of "object" transaction. SNMP operates on a table row level (and each object could potentially be represented with multiple rows in different tables).

#### **13.4.2.2 Architecture**

The Concentrator is located between the Central System and the Electricity Meter/Communications hub, and therefore needs to be interoperable at both interfaces. The Concentrator is expected to operate in one of three ways:

- As a network switch: The Concentrator only forwards requests to a particular meter and returns the responses;
- As a network router: The Concentrator has some intelligence regarding the grouping and de-grouping of meters;
- As a smart component: The Concentrator has specific intelligence for supporting smart meter functionality.

The Concentrator uses Web Services in combination with an XML Schema (XDS). The Web services include WS-Addressing, WS-Resource Transfer and WS-Eventing.

- WS-Addressing (wsa) is a standardized way of including message routing data within SOAP headers. This profile defines XML (XML 1.0, XML Namespaces) elements to identify Web service endpoints and to secure end-to-end endpoint identification in messages. This profile enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner.
- WS-Resource Transfer (WS-TR) is an extension to the WS-Transfer specification, which defines standard messages for controlling resources such as "get", "put", "create", and "delete". The extensions mainly deal with fragment-based access to resources.
- WS-Eventing defines a protocol for web services to subscribe to another web service, or to accept a subscription from another web service. It is used to provide asynchronous notifications to interested parties.

The Central System communicates to the Web Services server running on the Concentrator. The Concentrator can be requested to manipulated/read COSEM objects with a generic mechanism. These operations can be set for immediate execution, scheduled to future time execution or set for recurring execution.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**79/83

## 14 CI3 (Concentrator-Local O&M device)

### 14.1 Introduction

CI3 being the local O&M device interface for the Concentrator, it remains clear that the main cost driver for deciding on the type of profile is the type of Concentrator. Currently a broad range of Concentrators are expected in real AMI systems, depending on many factors (network topology, backbone technology, PLC technology over the MI1-CI1 interface, environmental constraints, etc.). Thus it is not in the scope of this document to provide a full description of all possible Concentrator types and their implication with respect to CI3 interface.

The proposed Data model and Application layer will be similar to the one already described for MI3.

HDLC is foreseen as one option, both with the RS232-C (i.e. V.24/V.28 specifications) and the optical port as described in [27] (§4.2 and §4.3).

Additionally, an Ethernet port is optionally proposed, so that COSEM APDUs are transported over the TCP/IP wrapper (see 7.3.4) and then IP datagrams encapsulated over Ethernet frames. The Concentrator and the local O&M device (usually a laptop) will need both RJ-45 Ethernet connectors.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**80/83

## 15 CI4 (Concentrator-External devices)

### 15.1 Introduction

There will be no gap analysis done and no research work (WP3) regarding CI4, as its implications are considered out of the scope of OPEN meter Project.

The interface CI4 is used to connect the Concentrator to external devices (e.g. sensors that are located in a relatively short radius around the Concentrator, power meters, etc.). PLC is not considered as an optimal solution from both installation and component perspectives.

Although [3] proposes wireless as a good alternative, the preferred Data model and Application layer (IEC 61850) is currently extensively used over wired Ethernet, and this is currently considered a good compromise solution for most applications. Given that the concept of External device is not fully defined in the scope of OPEN meter, the profile proposed here should not be considered as exhaustive.

### 15.2 Protocol assessment

IEC 61850 standards family was established in [2] as possible candidate for the CI4 interface, but no gap assessment was done in [3] because requirements would need further evaluation.

In recent years, the IEC 61850 standard family is extending its scope from primary substation to distribution networks and secondary substation level (more closely fitting CI4 interface in the System Architecture).

This technology could represent an opportunity in the incoming process of integration between protection, control, measurement and monitoring functions within the substation, taking advantages from the availability of Ethernet communications.

#### 15.2.1 Possible solutions

IEC 61850 uses OSI-7 layers stack for communication and divide messages in three groups as shown in the following scheme, where different types of messages are mapped into distinct communication stacks:

- *time critical* message: raw data samples and GOOSE<sup>1</sup> messages are directly mapped to low-level Ethernet layer in order to achieve improved performance by shortening the Ethernet frame and reducing the processing time. In addition, direct mapping on level 2 implies a higher security level than IP messages.
- *Client-server* messages: the command message with access control, the low speed message and the file transfer functions, are mapped to MMS protocol which has a TCP/IP stack above the Ethernet layer.
- *Time synchronization* messages are broadcasted using UDP/IP.

---

<sup>1</sup> Generic Object Oriented Substation Event: a mechanism for the fast transmission of substation events, such as commands, alarms, indications, as messages



**Energy Theme; Grant Agreement No 226369**

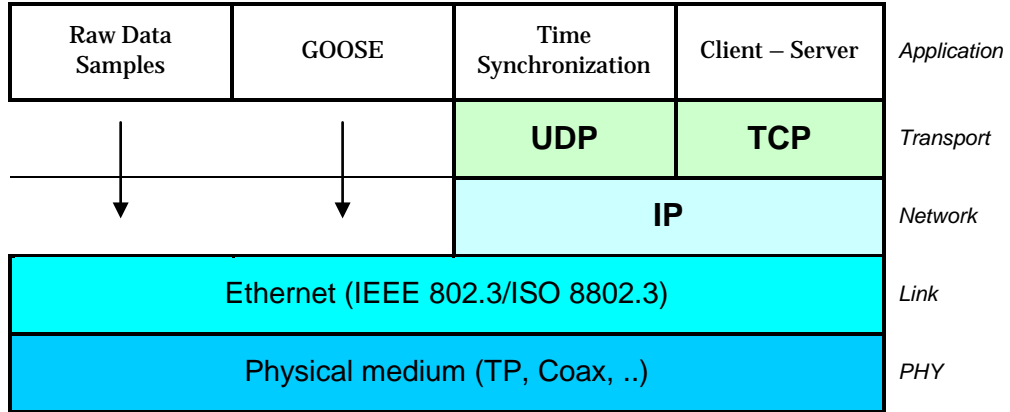


Figure 18 - IEC 61850 stack and messages

The following scheme outlines with more details possible combinations between upper and lower layers in current applications.

Table 8 - complete IEC 61850 stack and links with other standards

<b>Time Sync</b> SNTP	<b>Sample d Values</b>	<b>GOOSE</b> Generic Object Oriented Substation Event	<b>GSSE</b> Generic Substation Status Event (MMS ISO 9506 Connectionless ACSE ISO/IEC 8649,10035)	<b>Client-Server</b> (MMS ISO 9506 Core ACSE Services Connection-oriented ACSE ISO/IEC 8649,8650)		
n/a	n/a	ASN.1, BER ISO/IEC 8824.1	Connectionless presentation ISO/IEC 8649,10035 ASN.1, BER ISO/IEC 8824.1	Connection-Oriented presentation protocol ISO/IEC 8822,8823 ASN.1, BER ISO/IEC 8824.1		<i>Presentation</i>
n/a	n/a	n/a	Connectionless session ISO/IEC 9548	Connection-oriented session ISO/IEC 8326,8327		<i>Session</i>
UDP/IP	n/a	n/a	GSSE T-Profile ISO/IEC 8602	ISO CO T-Profile ISO/IEC 8073	TCP/IP T-Profile ISO Transport on top of TCP (RFC 1006)	<i>Transport</i>
IP (RFC 791)	n/a	n/a	ISO/IEC 9542	ISO/IEC 8473	IP (RFC 791)	<i>Network</i>
RFC 894	Priority Tagging / VLAN (IEEE 802.1Q)		ISO/IEC 8802-2 LLC	ISO/IEC 8802-2 LLC	RFC 894	<i>Link</i>



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture **Version:** 1.1 **Page:**82/83

	CSMA/CD (ISO/IEC 8802.3)			
	ISO/IEC 8802.3 Ethertype	ISO/IEC 8802.3	ISO/IEC 8802.3 Ethertype	PHY

(Source: <http://www.ipcomm.de/protocol/IEC61850/en/sheet.html>)

**15.2.2 Status of protocols**

IEC TC 57 is in charge for development of IEC 61850 family standards.

In the recent “NIST on the Smart Grid Interoperability Standards Roadmap”, published on August 2009, several extensions of IEC 61850 for distribution management applications are depicted.

See [www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf](http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf)

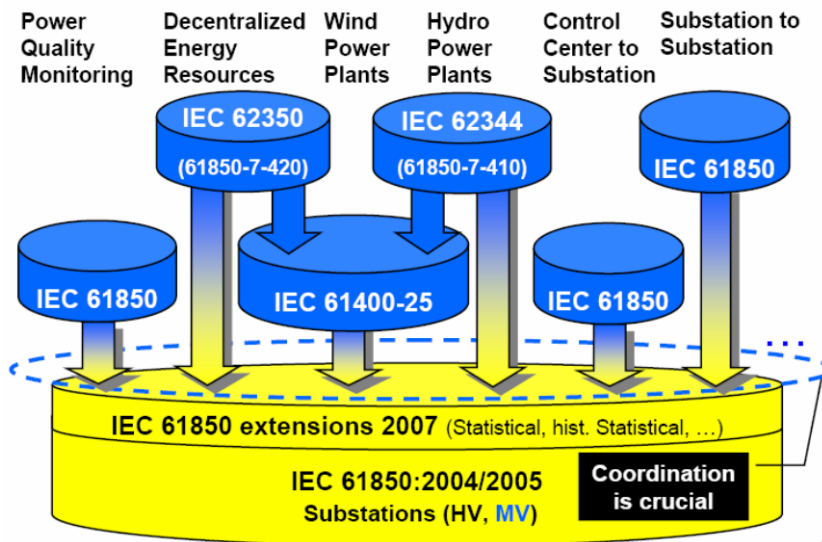


Figure 19 - IEC 61850 family and link with other standards

Efforts are focused on harmonizing IEC 61850 with the Common Information Model (CIM), which is described in IEC 61970 also as part of TC57 activities, for interfacing third-party applications (generally “advanced applications” such as improved power flow and contingency analysis), to an existing control center. Extensions of the Configuration Language to cover wind power and other distributed generators are under development. More recently IEC TC13 has started work with IEC TC57 to map DLMS/COSEM to CIM.

The website <http://iec61850-news.blogspot.com> provides up-to-date information about IEC 61850 development.



**Work Package:** WP3  
**Type of document:** Deliverable  
**Date:** 08/02/2010

**Energy Theme; Grant Agreement No 226369**

**Title:** Design of the overall System Architecture

**Version:** 1.1 **Page:**83/83

## 16 Copyright

*“Copyright and Reprint Permissions. You may freely reproduce all or part of this paper for non-commercial purposes, provided that the following conditions are fulfilled: (i) to cite the authors, as the copyright owners (ii) to cite the OPEN meter Project and mention that the European Commission co-finances it, by means of including this statement “OPEN meter. Energy Project No 226369. Funded by EC” and (iii) not to alter the information.”*