Pekka Koponen, Marja-Leena Pykälä, Janne Peltonen &
Pasi Ahonen

Interfaces of consumption metering infrastructures with the energy consumers

Review of standards

Interfaces of consumption metering infrastructures with the energy consumers

Review of standards

Pekka Koponen, Marja-Leena Pykälä, Janne Peltonen & Pasi Ahonen

Abstract

Standards for the data communication interfaces related to smart metering are reviewed in this report. The main focus is on the interfaces with the energy consumer's systems and appliances, but also the other interfaces are briefly discussed. Typically and increasingly these systems, meters and loads, such as appliances, are connected together via home automation or building automation networks. This interface is becoming increasingly important, because energy saving and demand response are needed more and more, and are enabled by the increase of intelligence in the electricity grids, houses and appliances. There are many protocols and standards, but the lack of a common open standard has delayed the development of the applications and services that depend on these interfaces. This may also have delayed the development of functional and interface requirements for the meters. The problem has been widely detected and there are ongoing initiatives to solve it. Also these initiatives are briefly discussed. It can be observed that many protocols have significant shortcomings regarding data security. This problem is outstanding especially with the home and building automation protocols.

Tiivistelmä

Tässä julkaisussa kartoitetaan energian kulutusmittausjärjestelmien tiedonsiirto-rajapintojen standardeja. Pääpaino on tiedonsiirrossa loppukäyttäjien järjestelmien ja laitteiden kanssa. Liitäntä tapahtuu yleensä ja enenevässä määrin rakennuksen tai kodin automaatioverkon kautta. Kyseisen liitännän merkitys on kasvamassa energiansäästön ja kysynnän jouston tarpeen sekä sähköverkkojen, talojen ja laitteiden älykkyyden lisääntyessä. Erilaisia protokollia ja standardeja on monia, mutta yhteisen avoimen rajapintastandardin puute on hidastanut kyseisistä rajapinnoista riippuvien sovellusten ja palvelujen kehittymistä. Tämä on voinut hidastaa myös mittareiden toiminnallisten ja rajapintavaatimusten kehitystä. Ongelma on yleisesti havaittu ja käynnissä on hankkeita, jotka pyrkivät ratkaisemaan sen. Myös näistä hankkeista keskustellaan lyhyesti. Havaittiin myös, että tietoturvan toteuttamista vaikeuttavat siihen liittyvät puutteet monissa protokollissa. Erityisesti koti- ja rakennusautomaatioon liittyvässä tiedonsiirrossa tämä on huomattava ongelma.

Preface

This report was done as a part of the Finnish national research project "Interactive customer interface for advanced distribution management and electricity market" INCA. It was funded by Tekes – Finnish Funding Agency for Technology and Innovation and the project partners.

A good starting point for this review was provided by the contributions of the authors in and the information received from 1) the European Smart Metering Alliance project, coordinator John Parsons, Beama 2) the Finnish national project on the data security of industrial automation systems TITAN (Tietoturvaa teollisuusautomaatioon), coordinator Pasi Ahonen, VTT, and 3) a Finnish national project "Open ICT based platform for energy efficiency evaluation of buildings" on eCertification, coordinator Jorma Pietiläinen, VTT.

Making a report in early 2010 on the development of smart metering after ESMA was included in the INCA project plan. In the summer 2009 the steering board of the INCA project and especially its members Matti Rae from ENSTO and Seppo Yrjölä from Nokia Siemens Networks emphasised that such a report is needed and it should have enough focus on standardisation and Home and Building Automation related issues.The INCA steering board also accepted increasing the resources allocated for this report by moving them from an other task. This made writing this review possible.

We also want to thank Petri Trygg of PowerQ, Timo Knuutila, Holger Elias and Juergen Heiles of Nokia Siemens Networks GmbH & Co. KG for many clear and useful comments that helped us make this report better. We are also grateful to PhD Pentti Uuspää for checking the language and some other details.

The authors

Contents

Abbreviations

AA	Application Association
ACSE	Application Control Service Element
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AMM	Advanced Meter Management, Automatic Meter Management
AMR	Automatic Meter Reading
AMRA	Automatic Meter Reading Association
ANSI	American National Standards Institute
APERAK	Application error and acknowledgement message of EDIEL
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BACnet	Building Automation and Controls network
BAFF	Building Automation Forum of Finland
BSI	British Standards, the National Standards Body of the UK
BWA	Wireless Broadband Access
CAN	Controller Area Network
CDMA	Code Division Multiple Access
CEFACT	See UN/CEFACT
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPCA	Consumer Electronics Powerline Communication Alliance
CIM	Common Information Model
CIP	Critical Infrastructure Protection
COSEM	COmpanion Specification for Energy Metering
CSA	Canadian Standards Association
CSS	Cascading Style Sheets by W3C
DCCP	Datagram Congestion Control Protocol
DHS	United States Department of Homeland Security
DIN	Deutsches Institut für Normung
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
DLMS	Device Language Message Specification

DNP3	Distributed Network Protocol
DSO	Distribution System Operator
DSS	Digital Signature Standard
DS2	Design of Systems on Silicon, a powerline communications chip-set developer
DTLS	Datagram Transport Layer Security
ebIX	European Forum for Energy Business Information Exchange
ebXML	Electronic Business using eXtensible Markup Language
EDIel	Electronic Data Interchange in electricity, standard based on UN/EDIFACT
EDIFACT	See UN/EDIFACT
EDGE	Enhanced Data Rates for GSM Evolution, known also as EGPRS
EDIgas	Electronic Data Interchange in gas, standard based on UN/EDIFACT
EDL	Exchange Data Language
EFET	European Federation of Energy Traders
EFTA	European Free Trade Association
EGPRS	Enhanced GPRS, known also as EDGE
EHS	European Home Systems, a standard for home automation networks
EIA	Electronic Industries Alliance, accredited by ANSI since 1984
EIB	European Installation Bus, part of KNX standard
EISA	Energy Independence and Security Act
ENTSO E	European Transmission System Operators
ERGEG	European Regulators' Group for Electricity and Gas
ERMES	European Radio Messaging System, a radio paging system
ESD	Energy end-use efficiency and Energy Services Directive
ESMA	European Smart Metering Alliance
ETSI	European Telecommunications Standards Institute
EURIDIS	EURIDIS association and protocol for reading of energy meters, standardised as IEC 62056-31
FLAG	FLAG protocol is a subset of IEC 62056-21 (former IEC 61107)
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications

GSM/GPRS	Global System for Mobile Communications / General Packet Radio Service
HAN	Home Automation Network, Home Area Network
HBES	Home and Building Electric Systems
HDLC	High-level data link control, protocol
HES	Home Electronic System
HFC	Hybrid Fiber/Coax
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPSec	Security Architecture for the Internet Protocol
IPSO	Internet Protocol for Smart Objects
IPTV	Internet Protocol TeleVision
ISO	International Organization for Standardization
ISOC	Internet Society
ISTEON	A network technology for home management and control
ITU	International Telecommunication Union, United Nations agency for information and communication technology issues
ITU-T	Standardization sector of ITU
KNX	A communications protocol for intelligent buildings (EN 50090, ISO/IEC 14543)
LAN	Local Area Network
LTE	Long Term Evolution, a beyond-third-generation mobile broadband standard
MAC	Medium Access Control
MDMS	Metered Data Management System
MID	Measuring Instruments Directive
MMS	Manufacturing Message Specification
NEMA	The Association of Electrical and Medical Imaging Equipment Manufacturers (National Electrical Manufacturers Association)
NEN	Netherlands Standardization Institute
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology

OASIS	Organization for the Advancement of Structured Information Standards
OBIS	Object identification system
oBIX	Open Building Information Exchange
OMS	Open Metering System
OpenAMI	Open Advanced Metering Infrastructure, refers to the OpenAMI task force sponsored by the UCA(R) International Users Group
OPERA	Open PLC European Research Alliance
PAMR	Public Access Mobile Radio
PCE	Parliamentary Commissioner for the Environment, New Zealand
PHY	Physical Access Control
PLC	Power Line Communication
PMR	Private Mobile Radio
PRIME	A narrowband PLC communication technology by PRIME Alliance, http://www.prime-alliance.org/
RAN	Radio Access Network
ReFLEX	A radio paging system
RF	Radio Frequency
RFID	Radio-Frequency Identification
RTO/ISO	Regional Transmission Operator / Independent System Operator
SAE	System Architecture Evaluation
SC	Standards Committee
SCTP	Stream Control Transmission Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Real-time Transport Protocol
SSPC	ASHRAE Standing Standard Project Committee
TC	Technical Committee
TCP/IP	Transmission Control Protocol / Internet Protocol
TDL	Table Description Language
TDMA	Time Division Multiple Access
TETRA	TErrestrial Trunked Radio
TF	Task Force
TLS	Transport Layer Security
TSO	Transmission System Operator

UCA	Utility Control Architecture
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Commerce
UN/EDIFACT	United Nations/Electronic Data Interchange For Administration, Commerce and Transport, standard
UPA	Universal Powerline Association
USNC	U.S. National Committee
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik
VHF	Very High Frequency
VLF	Very Low Frequency
WAN	Wide Area communication Network
W-CDMA	Wideband Code Division Multiple Access
WG	Work Group, Working Group
Wi-Fi	Wi-Fi Alliance that manufacturers may use to brand certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11
WiMAX	Worldwide Inter-operability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
W3C	World Wide Web Consortium
xDSL	Digital Subscriber Line
XML	Extensible Markup Language
ZigBee	A specification of a suite of communication protocols for WPANs.
3GPP	3rd Generation Partnership Project

1. Introduction

1.1 Background

Smart electricity grids and demand response are needed to make it possible to achieve the national and EU targets regarding power generation from renewable energy sources, distributed generation, energy efficiency and CO_2 emissions. There are also other related reasons such as improving the electricity retail markets and reducing the need to invest to network and peak power and reserve generation. Smart metering, also called advanced metering infrastructure AMI, is one of the enablers of the future smart grids and demand response. But this requires that the meters and the metering systems can at low cost provide adequate metering data and related functionality to the systems and services that need them. It is necessary to have common open standard interfaces in order to be able to get the benefits of scale that are necessary for achieving costs low enough. Standards help to reduce cost, improve competition and provide a more level playing field.

1.2 Objective and scope of the report

This report reviews the interface standards related to smart metering with emphasis on the interfaces connecting the metering infrastructure with the energy consumers, which are the customers in this context. There are many interfaces related to the smart metering infrastructure as shown in Figure 1. Thus the scope includes communication interfaces:

- from the smart metering system to home and building automation and home energy displays

- for metering related energy market communication with the energy consumers

- between the meter and the metering data collection interfaces, when it has some implications to the communication with the energy consumers

- for such demand response that is implemented via the smart metering system.

Thus, for example, demand response communication that does not use the metering system is now outside the scope.
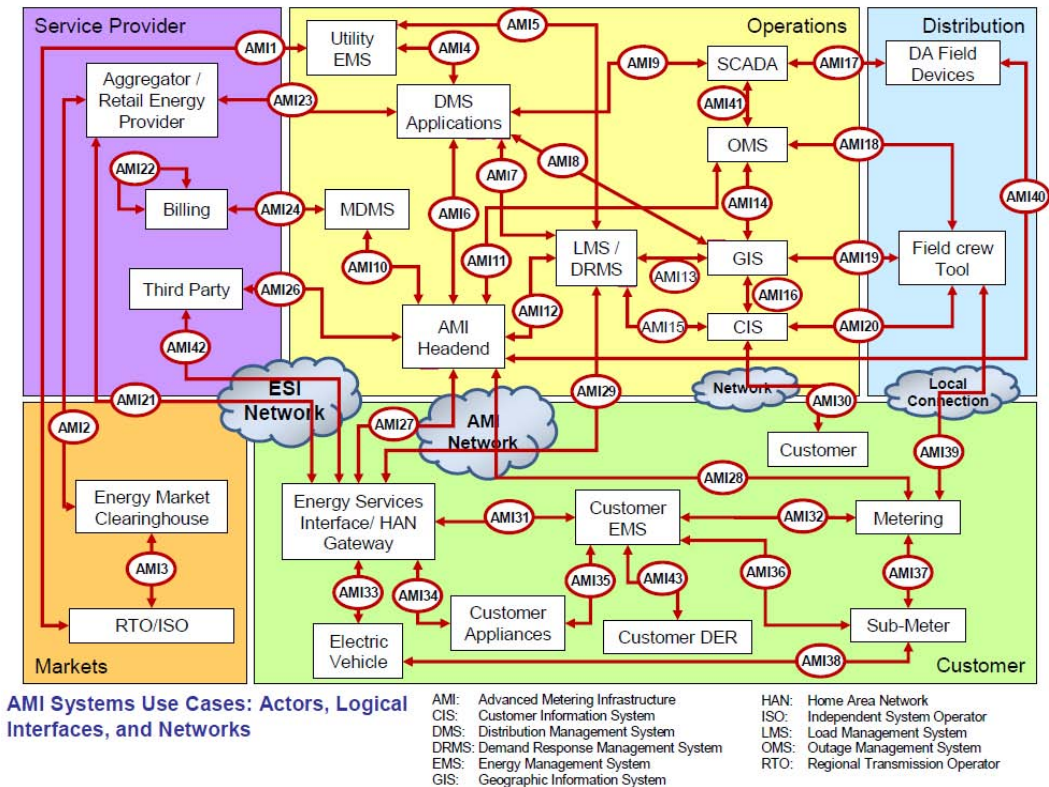
Figure 1. Advanced Metering Infrastructure Interfaces [NISTIR 2010].

In Figure 1 the abbreviation MDMS refers to Metered Data Management System. The other abbreviations are explained in Figure 1. Figure 1 describes the interfaces in the North American context. In the European context the RTO/ISO

should be replaced by TSO (Transmission System Operator). The focus of this report is on the customer related interfaces that are in the big green box down right in Figure 1. Thus there are 16 logical interfaces from the total of 43 that are within the scope.

Figure 1 shows the interfaces that can exist but not all of them are necessary in the same case. In Figure 2 there are less interfaces compared to Figure 1, because the scope is more limited and most connections go via a hub. The lowest part of Figure 2 is not within the scope now. An important interface is not explicitly shown in Figure 2. That is the interface that provides historical collected and analysed measurement data for the customer.
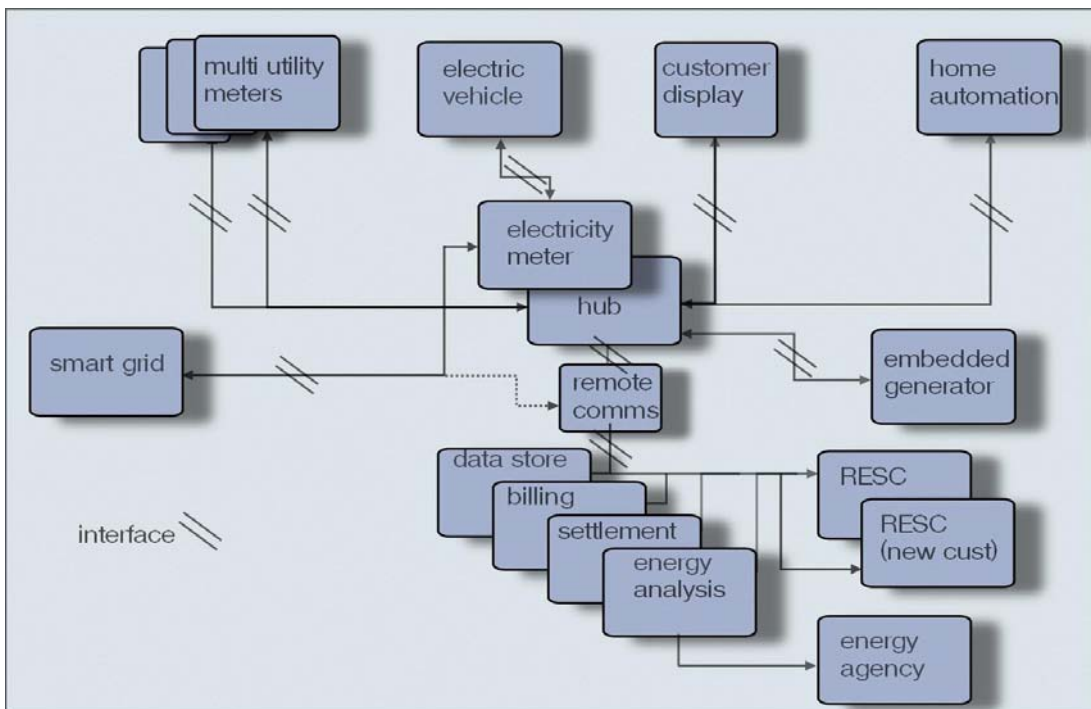
Figure 2. Interfaces across smart metering network [ESMA 2010], the abbreviation RESC (Retail Energy Supply Company) means the energy retailer.

2. Legislation and regulation

2.1 Sources of information

Chapter 11 of the European Smart Metering Guide 2010 [ESMA 2010] presents an overview of the regulatory and market conditions for smart metering in some European countries, and relevant topics regarding related standardisation. It concentrates on regulation of smart metering in the electricity sector, because mandatory implementation of smart metering of gas, water and district heating is still very limited. A comparative overview of legal framework related to gas and electricity metering is presented in [ERGEG 2007] and the status of regulatory aspects in [ERGEG 2009].

2.2 Relevant European directives

The two recent European Directives: [Directive 2004/22/EC] on measuring instruments (MID) and [Directive 2006/32/EC] on energy end-use efficiency and energy services (ESD) are important regarding smart metering in Europe. Also the Energy Performance in Buildings Directive [Directive 2002/91/EC] and the Commission's third legislative package for Electricity & Gas markets [EC 2007] include issues relevant to smart metering.

In addition the European Commission has issued a mandate, see [ESO 2009], to the three European Standards' Organizations (ESO) CEN, CENELEC and ETSI for the standardization of Smart Metering functionalities and communication for usage in Europe for electricity, gas, heat and water applications (M/441 – Annex 1). The objective is interoperability of technologies and applications within a harmonised European Energy Market. Mandate M/441 is ongoing and thus discussed more in the Chapter 10 of this report.

2.2.1 Measuring instruments directive (MID)

The measurement instrument directive (MID) [Directive 2004/22/EC] provides legal metrological control of most measuring instruments and thus aims to ensure that trade based on measurement is accurate, reliable and fair. The MID addresses the metrological aspects of the meters, such as minimum accuracy and the quantities that should be measured. But it also requires that measurement data relevant for the bill is displayed to the customer. It is illegal under European law for member states to impose additional requirements above the essential requirements of the MID. This will constrain the ability of Governments or national regulators to mandate detailed technical requirements for smart meters. Interpretation of this aspect is somewhat controversial, because 1) some strict interpretations related to the display issues are in practise clearly in conflict with the purpose of MID and ESD, and 2) because the EU legislation does not yet include such common requirements on the interfaces and functionality that are necessary for demand response and for enabling smart metering to give net benefits to the end customer and the society. However, purchasers of meters are free to specify additional meter functionality.

2.2.2 Energy Services Directive (ESD)

Article 13 of the Energy Service Directive [Directive 2006/32/EC] states the following:

"1. Member States shall ensure that, in so far as it is technically possible, financially reasonable and proportionate in relation to the potential energy savings, final customers for electricity, natural gas, district heating and/or cooling and domestic hot water are provided with competitively priced individual meters that accurately reflect the final customer's actual energy consumption and that provide information on actual time of use. When an existing meter is replaced, such competitively priced individual meters shall always be provided, unless this is technically impossible or not cost-effective in relation to the estimated potential savings in the long term. When a new connection is made in a new building or a building undergoes major renovations, as set out in Directive 2002/91/EC, such competitively priced individual meters shall always be provided.

2. Member States shall ensure that, where appropriate, billing performed by energy distributors, distribution system operators and retail energy sales com-

panies is based on actual energy consumption, and is presented in clear and understandable terms. Appropriate information shall be made available with the bill to provide final customers with a comprehensive account of current energy costs. Billing on the basis of actual consumption shall be performed frequently enough to enable customers to regulate their own energy consumption.

3. Member States shall ensure that, where appropriate, the following information is made available to final customers in clear and understandable terms by energy distributors, distribution system operators or retail energy sales companies in or with their bills, contracts, transactions, and/or receipts at distribution stations: (a) current actual prices and actual consumption of energy; (b) comparisons of the final customer's current energy consumption with consumption for the same period in the previous year, preferably in graphic form; (c) wherever possible and useful, comparisons with an average normalised or benchmarked user of energy in the same user category; (d) contact information for consumers' organisations, energy agencies or similar bodies, including website addresses, from which information may be obtained on available energy efficiency improvement measures, comparative end-user profiles and/or objective technical specifications for energy-using equipment."

2.2.3 The third energy package

The "Third Energy Package" of the European Commission includes Directive 2009/72/EC for electricity market and Directive 2009/73/EC for gas market [Directive 2006/32/EC, Directive 2009/72/EC]. They both require the implementation of "intelligent metering systems that shall assist the active participation of consumers in the … market". See Annex 2 (2) and also Article 3(11) in electricity and Article 3(8) in gas. 80% of electricity customers should have such meters by 2020. The member states decide the timeframe for roll-out of gas meters. Both of these Directives require that member states ensure interoperability of the metering systems to be implemented in their territories and have due regard to the use of appropriate standards.

2.3 National requirements

National requirements within Europe are considered as barriers for free trade and competition, but they have also been necessary in enabling development in de-

mand response and smart metering. European legislation has been so far slow to react and produce generic and adequate requirements that meet the emerging needs in different countries regarding smart metering applications including demand response and energy saving.

Thus there are national requirements regarding interfaces and functionality of smart metering systems in many countries within the European Union such as Finland, France, Italy, Ireland, the Netherlands, Spain and UK. Some examples are

- the Netherlands Technical Agreement number 8130, NTA 8130:2007

- the Finnish Electricity Market Act 65/2009 (Valtioneuvoston asetus sähkömarkkinoista 65/2009

  http://www.finlex.fi/fi/laki/alkup/2009/20090065)

- Italian national requirements [Villa 2007].

There are national requirements in countries outside Europe also such as Australia, and Ontario in Canada.

2.4 Legislation on data security and privacy

It is also necessary that the interfaces of smart metering systems are compatible with European and national legislation regarding privacy. For example BeAware project www.energyawareness.eu/beaware identified privacy laws at rule in the countries (Italy, Sweden and Finland), where users' data was planned to be collected in the BeAware project:

EU Data protection Law [Directive 95/46/EC and Directive 2002/58/EC]

Finnish Personal Data Act (523/1999)

Italian Privacy Law (Ds 196/2003)

Swedish Personal Data Act: Personuppgiftslagen (1998:204)].

Also in Germany there is legislation concerning data integrity and data security that is relevant regarding collection and use of metering data. In the Netherlands the smart metering concerns on data privacy have delayed the planned nation wide full penetration smart metering.

3. Standardization bodies

3.1 General

The most important international standardization bodies are ISO and IEC. ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 163 countries. IEC (International Electrotechnical Committee) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic, and related technologies.

CENELEC (European Committee for Electrotechnical Standardization) was created in 1973. Nowadays, CENELEC is a non-profit technical organization set up under Belgian law and composed of the National Electrotechnical Committees of 31 European countries. The development of smart metering standards in Europe is likely to be international and requires cooperation through the main European standards bodies; CENELEC, for electronic and electrical aspects, ETSI (European Telecommunication Standards Institute) for communications and CEN (European Committee for Standardization) for all other aspects.

IEEE (Institute of Electrical and Electronics Engineers) is the world's largest professional association advancing innovation and technological excellence for the benefit of humanity. IEEE has become active regarding the Smart Grids development and is able to provide the diversity of expertise, information, resources, and vision needed to realize the Smart Grids.

The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The Internet protocol suite and its ongoing development have an important role in enabling Smart Grids. A de-

scription of the core protocols of the Internet Protocol Suite as a response to guidance requested by NIST for Smart Grids discussion is now in http://tools.ietf.org/html/draft-baker-ietf-core-04.

The open internet standards and their development are an important enabler for various applications based on communication networks, including smart grids and smart metering. Protocols based on internet standards are increasingly applied in the communication and interfaces for smart metering between the physical communication technologies and the application level information models. The key internet standardisation organisations operate under the Internet Society (ISOC). ISOC and W3C announced a donation from ISOC for the purpose of advancing the evolution of W3C as an organization that creates open Web standards. ISOC is the organizational home of the Internet Engineering Task Force (IETF), the Internet's premier technical standards body.

National standardisation bodies have a role in the international standardization work, too. The American National Standards Institute (ANSI, www.ansi.org) has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system. In many instances, U.S. standards are taken forward to ISO and IEC, through ANSI or the USNC (U.S. National Committee), where they are adopted in whole or in part as international standards. For this reason, ANSI plays an important part in creating international standards.

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has over the past years formed expert working groups, assessed the current state of smart grid interoperability and that of stakeholder's planned activities and is building initial business-use cases. NIST launched in April 2009 its three phase plan to expedite development of Smart Grid interoperability standards for the U.S. electric power system. Under the Energy Independence and Security Act (EISA) of 2007, the NIST has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems…", www.nist.gov/smartgrid/ . NIST prepared a Smart Grid Interoperability Standards Roadmap [NIST 2010]. NIST has established the Smart Grid Interoperability Panel (SGIP) which drives and coordinates the Smart Grid standardization in various standardization bodies.

BSI British Standards is the UK's national standards organization that produces standards and information products that promote and share best practice. BSI has established the SMART METER Group SMG/1 to monitor the work of

the CEN/CENELEC/ETSI Smart Meter Co-ordination Group (SM-CG), to discuss UK interests and enable common views to be presented by UK-based members of the SM-CG.

The electrotechnical DIN standards (Deutsches Institut für Normung) issued by the DKE (Deutsche Kommission Elektrotechnik) are part of the German standards collection. These electrotechnical safety standards receive a VDE (Verband der Elektrotechnik Elektronik Informationstechnik) classification number and are included in the VDE Specifications Code of Safety Standards. DIN has in 2006 developed draft standard E-DIN 43863-4 for IP telemetry for meter data communication. DIN 43863-3:1997 defined identification codes for meter data that have been adopted by the IEC 62056-61:2006 standard.

3.2 Standardization in building automation

In the field of building automation and control systems (BACS) standardization is needed to reduce trade barriers, to open markets, to create competition between companies, and to allow the independence of building owner from constructor and manufacturer. It is also important to decrease investment and life-cycle costs of the building owner, and to decrease design costs and to be basis for sustainable system integration.

Main standardization committees in the field of building automation for non-residential buildings are CEN/TC 247 Building Automation, Controls and Building Management, ISO/TC 205 WG3 Building Control System Design, and ANSI/ASHRAE SSPC 135. Regarding residential buildings the corresponding standardization committees on European level are CENELEC/TC 205 Home and Building Electric Systems (HBES), and IEC/ISO JTC 1/SG 25/WG 1 Home Electronic System (HES).

ISO/TC 205 is creating a system of International Standards to address the 'built environment', and is initially limiting the application of its International Standards to commercial and institutional environments. The main areas of work covered by ISO/TC 205 are:

1. The design of energy-efficient buildings

2. Building control systems design

3. Indoor air quality

4. Indoor thermal environment

5. Indoor acoustical environment

6. Indoor visual environment.

ISO/TC 205 WG 3 Building Control System Design workgroup is responsible for the global standardization of building automation. ISO has approved KNX, LonWorks, and BACnet as international standards (discussed in Chapter 8.1). The standardization work is done jointly with CEN under the Agreement on technical cooperation between ISO and CEN. [ISO 2010]

ISO/IEC JTC 1/SC 25/WG 1 produces standards for "Home Electronic System", that is for control communication within homes. This scope includes the control of equipment for heating, lighting, audio/video, telecommunications, security etc. It also includes residential gateways between the internal Home Electronic System network and external wide-area networks such as the Internet. The group also looks at similar building management functions in commercial buildings. A major focus of interest has become home and building energy management and connection to the smart grid. [ISO 2010]

CEN/TC 247 develops European standards for Building Automation, Controls, and Building Management for residential and non-residential buildings. CEN/TC 247 work is organized to several workgroups:

- WG 3: Building Automation and Control Systems

- WG 4: Open Data Transmission

- WG 6: Electronic control equipment for HVAC applications, integrated room automation, controls and management systems

- JWG CLC/TC205-CEN/TC247: Safety and Security.

From the information systems point of view, the most interesting workgroup is WG4 Open Data Transmission, which develops data transmission standards for building automation systems. WG4 has approved standards for KNX, LonWorks, and BACnet technology. The workgroup has also worked out some standards in cooperation with ISO. [CEN 2010]

CENELEC/TC205 Home and Building Electric Systems (HBES) prepares standards to ensure integration of a wide spectrum of control applications and the control and management aspects of other applications in and around homes and buildings, including the gateways to different transmission media and public networks taking into account all matters of EMC and electrical and functional

safety. TC 205 will not prepare device standards but the necessary performance requirements and necessary hardware and software interfaces. The standards should specify conformity tests. TC 205 will perform the work in close co-operation with relevant CENELEC TCs and those in CEN and ETSI. [CENELEC 2010]

The standing standardization program committee ANSI/ASHRAE SSPC 135 develops and maintains the BACnet standard. The American Society of Heating, Refrigerating and Air-Conditioning Engineers advances technology to serve humanity and promote a sustainable world. The actual work of SSPC 135 is taken care by its working groups. The most interesting workgroup is the UI-WG: Utility Integration. The scope of UI-WG is to Research, draft, and propose additions to the BACnet standard to support communications between building automation and control systems and public utility providers. The group will build from the work of ASHRAE Research Project 1011. Example application topics are real-time price negotiation, load management, and metering. [ASHRAE 2010]

ITU-T is the Telecommunication Standardization Sector of ITU, the United Nations agency for information and communication technology issues. ITU-T produces and revises standards (ITU-T Recommendations), covering everything from core network functionality and broadband to next generation services. The ITU-T group working on home networking specifications under the G.hn banner has agreed on some specifications for smart grid products such as smart meters, plug-in electrical vehicles, smart thermostats, smart household appliances and in-home displays. Demand response and advanced metering are among the target applications. G.hn is a next generation wired home networking standard developed by ITU-T, which supports high-speed communication over power lines, phone lines and coaxial cable. [ITU-T 2010]

The next Figure 3 describes the current networking activities between different organizations.
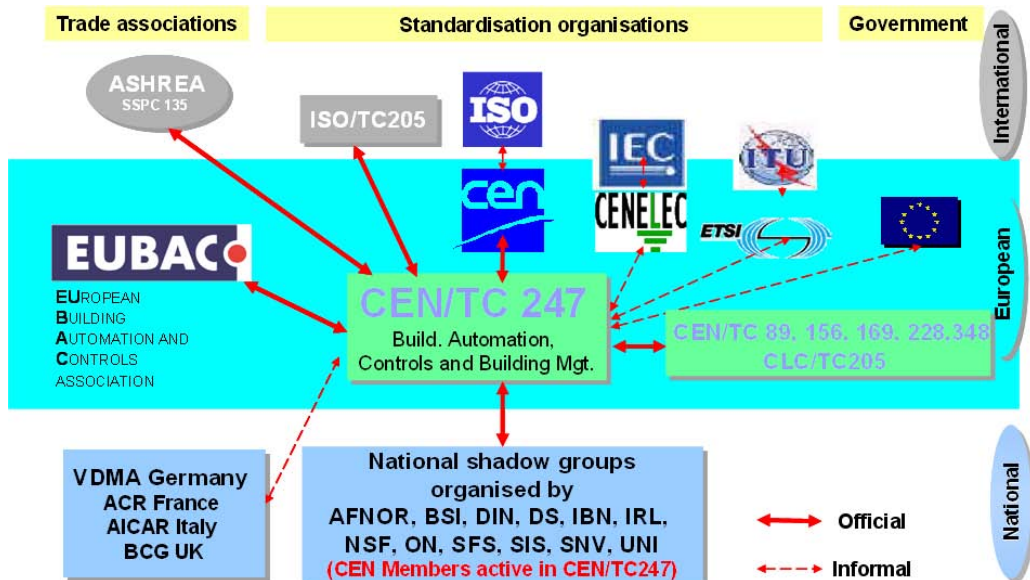
Figure 3. Networking activities between different organizations [CEN 2010].

In the European scope, the authors of this document see that ISO TC 205 and CEN/TC 247 are the most potential organizations to take further the standardization work in the area of building information and building automation systems standardization. They are able to deal with smart metering network aspects in home as well as buildings. Finally, there are still a considerable number of standards that relate primarily to building automation, controls and building management, and are only indirectly relevant to smart metering. They have not been considered in the scope of this document.

Often the early phases of the development of a standard happen outside established standardization bodies. An example is the ZigBee/HomePlug Smart Energy Profile 2.0 that is a communication and information model for Home Area Networking. The profile is under development by a joint working group of the ZigBee Alliance and the Home Plug Alliance. It is said to be based on IP, and anticipated to be open and useful for many smart grid applications.

3.3 Standardization in power system control communication and consumption metering

IEC technical committees TC 13 and TC 57 have prepared standards related to electrical energy measurements as well as power systems control and communication.

The technical committee TC has issued over 50 publications within a field of equipment for electrical energy measurement, tariff and load control, customer information, payment, local and remote data exchange. 17 standards listed in the references are closely related to interfaces.

The IEC TC 57 Technical Committee has standardised communication protocols for different aspects of utility communication. These include various and specialised IEC 60870 protocols and more modern and ubiquitous IEC 61850 protocols applied now mainly within sub-stations, and the Common Information Model (CIM) protocols IEC 61970 / IEC 61968 for DMS/EMS Systems as well as Enterprise Integration for connecting data between utility systems and ERP, Asset Management, Trouble Call Management, and between Different Energy Participants and System Operators (SO). The TC 57 working group also has adopted the DLMS / IEC 62056 as the standard for metering. The object oriented IEC 61850, IEC 61968 and IEC 61970 protocols and protocols based on them are globally gradually replacing many protocols including the IEC 60870 protocols still applied widely in Europe and the DNP3 (Distributed Network Protocol, www.dnp.org) protocol that is very popular in North America in device level communications and interfaces, and many proprietary power network automation protocols. IEC 61850 is considered to be better than DNP3 for smart grids and mapping between DNP3 data objects to IEC 61850 information objects is being led by NIST [NIST 2010, p. 95–96]. Also the IEC protocols for communication with distributed energy resources are based on IEC 61850. It can be expected that future meter reading and metered data protocols will be developed to be compatible with IEC 61850 and CIM. That would reduce the need for conversion of metered data between protocols.

MultiSpeak (http://www.multispeak.org) was created by the National Rural Electric Cooperative Association (NRECA) and is used in the U.S.A. by many small rural electric utilities for information exchange regarding distribution automation, an area covered by IEC 61968. Thus also MultiSpeak can be expected to eventually converge to the global CIM. IEC TC57 WG14 and MultiSpeak have already agreed to collaborate. See also [NIST 2010, p. 93–95.] Mul-

tiSpeak provides interoperability more quickly than CIM, but it has fewer features and is much more difficult to expand. MultiSpeak also includes exchange of metered data.

IEEE-SA SCC21, IEEE-SA SCC31, IEEE-SA SCC36 (IEEE-SA = the Institute of Electrical and Electronics Engineers Standards Association), ANSI C12, NEMA (The Association of Electrical and Medical Imaging Equipment Manufacturers, www.nema.org), DLMS User Association (www.dlms.com), AMRA and OpenAMI are examples of the standardization bodies and user groups responding to the development needs of the standards related to metering. NEMA has participated in the development of ANSI C12 metering standards.

In order to address the challenges related to harmonization of metering and enabling energy end-use efficiency and feedback with smart metering, the European Commission and EFTA addressed Mandate M/441 to CEN, CENELEC and ETSI. A Smart Meters Coordination Group (SM-CG) was set up to answer this request concerning smart meter standardization issues.

NIST initiated the Smart Grid Interoperability Panel (SGIP), http://colla borate.nist.gov/twiki-sggrid/bin/view/SmartGrid.SGIP, which is both a forum for discussing smart grid technical issues and a collaboration to respond to these issues and to address emerging requirements for smart grid standards. The SGIP will further develop the initial NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 [NIST 2010]. There the PAP 05 (Priority Action Plan 05) focuses on defining new standard data profiles for meter data and publishes them as a new revision of the ANSI C12.19 standard. PAP 05 collaborators are AEIC (Association of Edison Illuminating Companies) ANSI C12 SC12.1 and C12 SC17 WG4, IEC TC 13 and TC57 Smart Grid TF, IEEE SCC31, MultiSpeak, NEMA, UCA International Users Group AMI-NET TF, Measurement Canada.

4. Actors and logical interfaces

Figure 1 in the Chapter 1 "Introduction" shows actors and interfaces relevant to the Advanced Metering Infrastructure (AMI) or smart metering. In the competitive energy market the network operations are unbundled from the power generation and electricity market businesses. As a result metering is related to many actors.

The most relevant actors here are:

1. Energy customer who consumes energy but may also provide flexibility of demand (demand response, via controllable loads and energy storage) and embedded generation to the grid; for the energy customers smart metering plays an important role in enabling the consumption to respond to fast price variations in the electricity markets and providing both historic and immediate feedback needed for energy saving.

2. Distribution network operator, who in most countries is also responsible for metering the consumption for billing; in the operation of the future smart grids with much distributed generation the distribution network operator needs to have possibilities to control the demand and distributed generation during those few periods when network capacity to transfer power would otherwise be inadequate.

3. Metering operator who operates the meter management system (AMM) and possibly also the metered data. Increasingly network operators outsource metering.

4. Energy retail company (often called as supplier in the energy retail market context) who sells energy to the final customers; the energy retail company also buys and sells energy and flexible (controllable) power in the wholesale market and retail market in order to minimise balancing

costs and maximise net profit; smart metering makes it possible to purchase flexible power from the retail customers and distributed generation.

5. Aggregator of distributed energy resources who aggregates the responses of distributed energy resources to provide demand response services for the actors of the energy wholesale markets and to the network and system operators; one of the main ideas is that the aggregator can get flexibility cheaper from the retail customers than from the wholesale market; the aggregator business can be part of the activities of some other energy market actor such as an energy retail company or energy service company, because this often brings synergy benefits. On one hand it is important for the energy retailer to predict and tune his actual balance to meet the commercial balance accurately and aggregation improves the predictability and flexibility of the loads. On the other hand the aggregator benefits from having the energy market tools and large customer and market portfolios of the energy retailer. For small distributed energy resources the costs of data communication and metering still tend to be too high compared to the benefits of aggregation, but smart metering is expected to change this by providing interval metering and transmission of load control signals.

6. Providers of services based on metered data; smart metering systems are expected to provide much of this data,

   o   data analysis services (energy efficiency analysis, power quality analysis, analysis of load curves and control responses, analysis of contracts)

   o   energy efficiency services to improve the energy end use efficiency and energy management and to promote energy saving

   o   monitoring services related to building management, safety and security, diagnostics such as detection of water or energy leakage, elderly care, etc.

7. Regulating authorities who monitor the performance of the network operators; for this they need data regarding power quality and outages at the customer connection points from the smart metering systems; in addition also metering is regulated by the authorities.

In Figure 1 most of the above actors (except the customer and the network operators) are grouped together as service providers and the metering operator as belonging to operations of the network. This indicates that in the context of that report the same interfaces with the other actors are considered sufficient for all of them. Here the context is different and this assumption needs to be reconsidered to some extent. Figure 4 illustrates the main actors, use cases and interfaces related to smart metering and energy consumer.
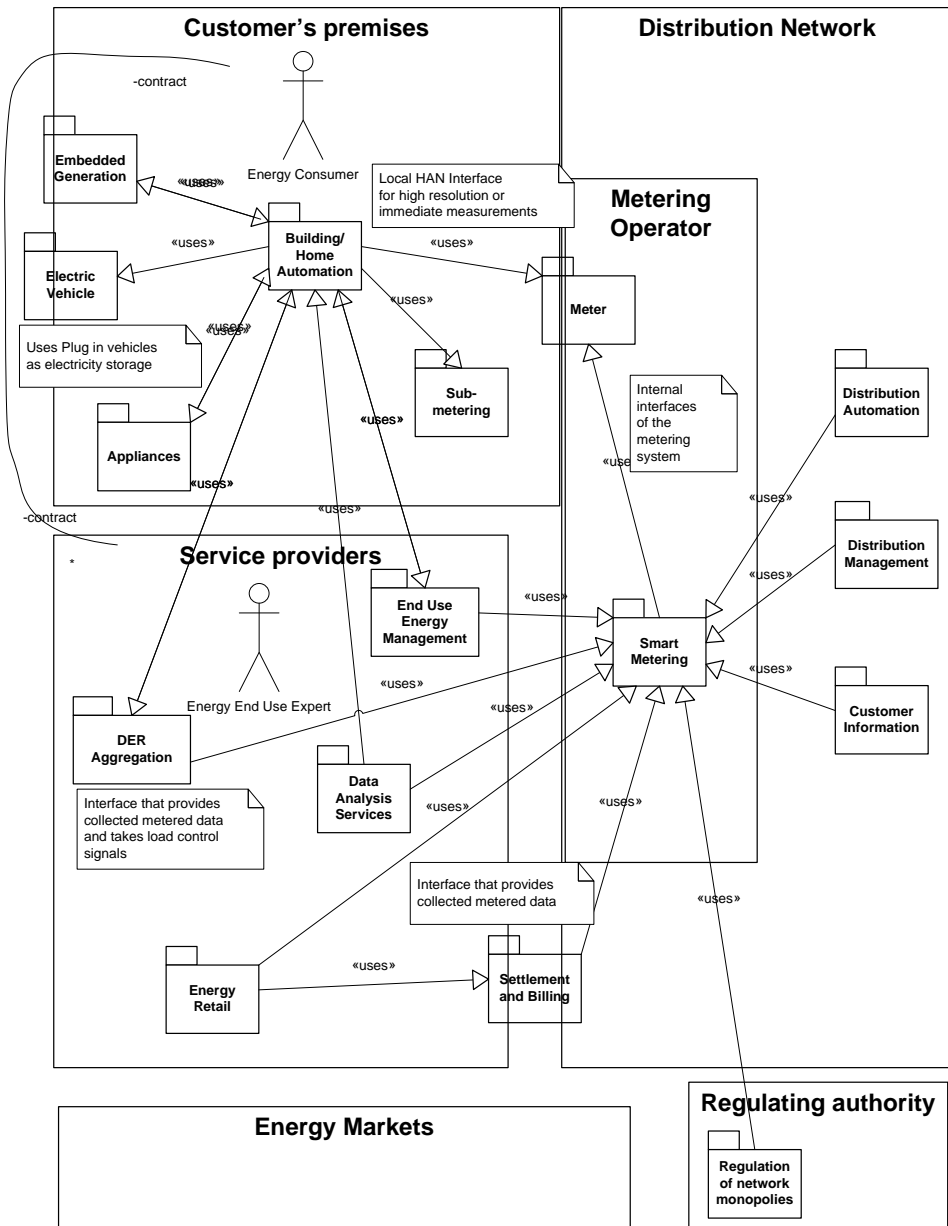
Figure 4. Main actors, use cases and interfaces related to smart metering and energy consumer.

5. Metering systems

5.1 Functionalities and challenges of metering systems

The functionalities that need support from the metering systems include

- provision of metered data for **balance settlement** in the electricity markets

- meter reading services

- customer information services

- power quality monitoring

- load control and demand response

- energy feedback and saving

- load and response modelling

- possible other functionalities that need metered data.

In order to meet the requirements of these functionalities certain other functionalities are also needed such as data security, authentication, connectivity management, meter management and installation management.

It is a substantial advantage, if the metering system can use multiple existing protocols and technologies to get the best fit with the local circumstances and adopt new ones when they meet the cost and performance requirements better than the existing ones. Services need to be delivered to many actors. Interoperability is important. Thus standardized open interfaces and also internet connectivity are needed.

5.2 Internal structure of metering systems

The metering systems has a central data and meter management system that communicates with the meters via a wide area communication network (WAN) for reading and managing the meters and for loads control purposes. Either the meters directly or data concentrators have WAN access such as a GSM/GPRS modem, xDSL-modem or satellite phone modem. If concentrators are applied then they communicate with the meters using some last kilometre communication technology such as PLC or short range RF communication. It is also possible that concentrators are situated in the same buildings with the meters and use there communication technologies suitable for the purpose.

The structure described above is characteristic for smart metering that is also called advanced metering infrastructure (AMI). In some countries there are also AMR systems where only part of the meter reading process is automated and the meter reading cars drive by the meters around the neighbourhoods collecting meter data with short range RF technologies, but these are not considered here, because the focus is in the future and because such systems are not applied in Finland in any significant scale.

5.3 Technologies and standards applied within metering systems

5.3.1 Overview of meter reading protocols

Europe

A communication protocol widely used for meter reading in the European Union is IEC 61107 that now is IEC 62056-21. It is a half-duplex protocol that uses ASCII data and a serial port such as a twisted pair EIA-485 (formerly known as RS-485) or an optical port. FLAG protocol is a subset of IEC 61107 that leaves less room for vendor specific features, see www.theflagprotocol.com. IEC 61107 is not an application layer protocol and vendor specific application layers are still often used with it.

IEC 62056 series of standards is a more modern and more complete meter reading protocol increasingly applied in Europe. It is called DLMS or Device Language Message Specification and has been developed and is maintained by

the DLMS User Association www.dlms.com . The IEC TC 57 Working Group 13 has adopted the DLMS / IEC 62056 as the standard for metering. DLMS standardises the communication profile, the data objects and the object identification codes and supports different communication media including Ethernet TCP/IP. The DLMS also provides for a conformance standard that helps manufacturers and utilities to ensure that suppliers comply with the standard.

The IEC 62056 "Electricity metering – Data exchange for meter reading, tariff and load control" comprises the following standards:

- IEC 62056-21: Direct local data exchange describes how to use COSEM over a local port (optical or current loop)

- IEC 62056-42: Physical layer services and procedures for connection-oriented asynchronous data exchange

- IEC 62056-46: Data link layer using HDLC protocol

- IEC 62056-47: COSEM transport layers for IPv4 networks

- IEC 62056-53: COSEM Application layer

- IEC 62056-61: Object identification system (OBIS)

- IEC 62056-62: Interface classes.

IEC 62056-21 is the same as the latest edition of IEC 61107. COSEM stands for Companion Specification for Electricity Metering. The DLMS/COSEM specification is standardised by both the IEC and CEN. The DLMS User Association www.dlms.com defines the protocols and provides its specification as three technical reports named Green Book, Yellow Book and Blue Book. The blue book describes the COSEM identification system and interface objects, the green book the COSEM three layer connection oriented architecture and the yellow book the COSEM conformance test tool specification. In addition to the IEC 62056 for electricity metering the DLMS/COSEM is also used in the EN 13757 standard series for gas, water, and heat metering.

The IEC 62056 allows the use of ANSI C12.19 data tables and most IEC 62056 meters in Europe are actually ANSI C12.19 compatible. The North American ANSI C12 standards are discussed next.

North America

In North America ANSI C12 standards for metering protocols are used instead of the IEC 62056 standards used in Europe. These standards are:

- ANSI C12.18: Protocol Specification for ANSI Type 2 Optical Port

- ANSI C12.19-2008: Utility Industry End Device Data Tables

- ANSI C12.21: Protocol Specification for Telephone Modem Communication

- ANSI C12.22: Protocol Specification for Interfacing to Data Communication Networks.

The standards corresponding to the IEC 62056-21 (IEC 61107) protocols are in North America the ANSI C12.18 for optical ports and ANSI C12.21 for modems.

Some remaining interoperability challenges

Some problems remain with the interoperability of DLMS/COSEM (IEC 62056) meters and systems such as 1) inadequate compatibility to IEC CIM (IEC 61970, IEC 61868 and IEC 61850), 2) possibility to use proprietary extensions and 3) the observed practise of meter system vendors to introduce minor incompatibilities that limit interoperability. Same kind of problems can exist also between systems and meters based on the ANSI C12 standards. The two last mentioned problems can be addressed by the certification process and by the purchase contracts of the meters and systems. The first mentioned problem can gradually diminish via standards harmonization.

5.3.2 Application layer protocols

Europe

The DLMS/COSEM standard metering object identification system IEC 62056-61 (OBIS) enables every meter reading system to understand a value by its identification system, irrespective of the meter. The DLMS/COSEM also allows for uploading the objects supported by a meter, and then reading the meter values,

which enable any DLMS/COSEM Compliant Client software to read any manufacturer's meter.

IEC 62056-53:2006 specifies the COSEM Application layer. It defines services for establishing and releasing application associations, and data communication services for accessing the methods and attributes of COSEM interface objects, defined in IEC 62056-62.

IEC 62056-62 specifies interface classes of a meter. It specifies a model of a meter as it is seen through its communication interfaces. This model is completely independent from the protocol layers used for transporting the data. Generic building blocks are defined using object-oriented methods, in the form of interface classes to model meters from simple up to very complex functionality. The interface class definitions standardise meter functionalities, such as demand registration, tariff and activity scheduling, handling time synchronisation and power failures, some power quality metering, and secure access to selected portions of the information at the metering equipment. In addition to electricity, it supports gas, water, and heat measurements.

North America

In North America ANSI C12 standards for metering protocols are used instead of the IEC 62056 standards used in Europe. The ANSI C12.19 standard presents common structures for encoding data in communication between end devices (meters, home appliances, ANSI C12.22 nodes) and utility enterprise collection and control systems using binary codes and XML content. The tables support gas, water, and electric sensors and related appliances. A comprehensive revision 2008 includes new tables, XML-based table description language (TDL/EDL), and the documentation of services and behaviours. It also features new and updated procedures, controls, and definitions. According to [NIST 2010, p. 78], a new major revision is being prepared and it is planned to be published in July 2010. This will include defining the common meter data tables that are required to enable smart grid applications such as demand response and real time usage information. ANSI C12.19 has a mechanism so support description of the tables, termed Exchange Data Language (EDL) which can be used to constrain new features into a well known form.

ANSI C12.19-1997 was developed collectively by the ANSI C12, Industry Canada and IEEE SCC31 to be one North American standard for metering data description. NEMA participates in the development of the ANSI C12 standards.

The ANSI C12.22 standard provides for meters a common application layer (layer 7 in the OSI reference model). It describes the process of transporting ANSI C12.19 table data over a variety of networks. ANSI C12.22 provides both session and sessionless communications, and also many application layer services. It uses AES encryption and it is also extensible to support additional security mechanisms.

Diverse

Near the ends of the metering systems some other protocols may be applied instead of the above mentioned meter reading standard protocols.

One case is connecting meters locally to a meter reading data concentrator or a main meter that may communicate upwards using the above mentioned standards; the reason typically is minimisation of data communication capacity needs and costs together with technologies with limited throughput. For the same reason the protocols applied in this area did not have clearly distinct application data profiles and application layer independent from technologies at the lower layers. LonMark profiles and some proprietary protocols are examples of such dependencies. There are also adequately layered protocol stacks applied for this purpose. Specifically for metering developed well layered bus-technology is M-bus EN 13757-3 that can use data content definitions for heat meters standardised in EN 1434-3:2008 or other application data definitions. Such definitions can be COSEM or ANSI C12.19, for example, and these have also been used for local communication of metering systems over existing local communication and automation networks built for other purposes, including Ethernet networks and the CeBUS home automation standard (EIA-600). A recent development is the ZigBee/HomePlug Smart Energy Profile SEP2.0 that will define an application layer and data model for smart grid support and thus for metered data and demand response.

Because it is necessary to transfer metered data across systems and organisations, and adequate standards have been missing, different national open protocols have been developed in various countries for the transfer of metered data and/or equipment parameterisation over stateless, secure communication paths. Examples are ODEL v.2 (Object oriented Data model for ELectricity supply) in

Norway and Smart Message Language (SML) in Germany. Now in this area both IEC CIM and the XML-based electricity market protocols may be preferred, because they are much more widely known, applied and supported.

5.3.3 TCP/IP

Also in smart metering there is a trend towards using TCP/IP. One reason for this is that the application layers should be independent from the physical communication and thus enable the use of many communication technologies. Another reason is that TCP/IP is ubiquitously applied everywhere and thus well developed and well known. In addition a unified network management system can be used all over the IP network. Such companies as Cisco and DS2 promote IP based smart grids communication platform that spans up to the homes of the energy customers. IP v.6 can much better support the communication needs of smart grids and demand response than IP v.4.that suffers from limited address space, lack of prioritising, poor suitability for energy efficient communication technologies etc.

5.3.4 Standards applied at the lowest layers of the protocol stack

The technologies and standards applied at the lower protocol stack levels (physical PHY and media access MAC) in the meter reading systems are well covered in the Deliverable D2.1/ Part 1 of the Open Meter project [OPENmeter] and in the ESMA Smart Metering Guide [ESMA 2010]. Also [Li 2008] discusses communication technologies for meter reading. Information from these sources is summarized and completed here.

WAN communication

2G/2.5G GSM/GPRS/EDGE

Today, mobile telephony services are available almost everywhere. Thus they are commonly used for AMR, also. SMS messages, circuit switched GSM data services or packet switched GPRS (General Packet Radio Service) or EGPRS (EDGE) data services are used for AMR depending on the system. It is common that the packet switched connections are closed when there is no need to communicate with the meters. Thus there is often a rather long delay associated with

the opening of the connection even when packet switched technologies are used. For fast load control purposes most mobile network based WAN communication systems are far from optimal due to long and varying latencies associated with the broadcasting of load control signals. GSM/GPRS/EDGE has good coverage and communication costs can be low, but the modems are still relatively expensive.

3G UMTS

3G/UMTS can provide data-only services. These are normally packet oriented and IP based. 3G/UMTS is increasingly providing broadband Internet access especially in those areas that are not served by xDSL and cable. Indoor penetration at 2 GHz is worse than at 900 MHz thus requiring house gateways or 2 GHz antennas to be mounted at well selected positions. Another drawback is that higher bandwidths consume more energy thus making it necessary to shut down the communication network faster during power interruptions.

LTE

The main advantages with LTE are high throughput, low latency, and plug and play. LTE will support seamless connection to existing networks, such as GSM, CDMA and WCDMA. However LTE requires a completely new radio access network (RAN) and core network deployment and is not backward compatible with existing UMTS systems.

The 3GPP (LTE) is defining IP-based, flat network architecture as part of the System Architecture Evaluation (SAE) effort. LTE–SAE architecture and concepts have been designed for efficient support of mass-market usage of any IP-based service.

TETRA

TETRA (TErrestrial Trunked Radio) is a European digital radio standard originally developed in ETSI for all sorts of Private Mobile Radio (PMR) and Public Access Mobile Radio (PAMR) applications such as police, ambulance, fire, transport and security services. TETRA uses time division multiple access (TDMA) technology with four slots on one radio carrier and 25 kHz carrier spacing. Because TETRA has been designed to support the PAMR applications,

it can also support control applications somewhat better than GSM/GPRS. But nation wide TETRA systems are reserved for public safety and emergency services and there is no public TETRA infrastructure. Due to small numbers the modems and mobile phones are also expensive compared to the more widely applied mobile phone technologies. In addition the application of TETRA and related technologies is not homogenous in Europe.

2-way radio paging (ERMES, ReFLEX)

Paging systems are typically operated at VHF e.g. 138 MHz, providing good penetration into buildings. Data rates are rather limited. Some paging standards also support 2-way communication. Since operation of paging systems have been discontinued in many areas, they cannot be considered as attractive for remote metering and related applications.

European Radio Ripple control

European Radio Ripple control system is presently used in Germany, Hungary, and possibly in some nearby countries for load control and customer tariff switching. It is unidirectional so it cannot replace two way communication technologies but can complement them by providing fast broadcast of control commands and tariff changes. It operates at VLF bands so the data rate is rather limited. The range of a single transmitter typically covers a radius of 300–500 km.

Satellite communication

Satellite systems for metering and energy related end-user services can be attractive in areas where there is no suitable terrestrial communication infrastructure or when a redundant communication channel is needed due to some critical services. Iridium and SpaceChecker provide such satellite based data communication networks.

Last kilometre communication

The technologies used for WAN access are discussed here. The technologies used inside the buildings are discussed later in Chapter 7.2; those technologies are used in building automation networks and home automation networks or

within the metering system for in-house communication with the meters and concentrators located in the same building as the meters. This division is not exact, because some technologies can be applied in both to some extent.

WLAN/WiFi (IEEE 802.11)

There are some cases where IEEE 802.11 WLAN/WiFi networks are applied in reading meters remotely. In the US, several cities (e.g.Santa Clara, CA) already use WLANs to automatically collect readings from electricity, gas, and water meters. Coverage in basements at frequencies above 2 GHz is poor so WLAN-based AMR solutions require meters or data collector gateways mounted above ground level outside of houses.

WiMAX (IEEE 802.16)

WiMAX (Worldwide Inter-operability for Microwave Access) is a Wireless Broadband Access (BWA) technology. It provides transmission speeds up to 72 Mbit/s in both directions and supports point-to-point and point-to-multipoint network topologies and a multitude of transmission modes and bandwidths to adapt to the different propagation conditions and user demands. The communication range is a few kilometres, except along a line of sight much longer distances are possible. Thus WiMAX is a wireless alternative to xDSL and other wired local access (last km) solutions.

Narrowband PLC

Power Line Communication (PLC) has been applied for several decades in Automatic Meter Reading. It is widely used in Europe and in America. In mass rollouts it enables low cost implementation and operation of meter reading systems in urban and suburban areas where customer density is not low. But power line communication has its problems. Its signals cannot go through transformers. It is relatively vulnerable to the disturbances, disturbance filters and changes in the loads and network in low voltage distribution networks. Increasing signal levels is sometimes used as a solution, but that increases also disturbances emitted to sensitive customers. As household appliances do not have strict electromagnetic compatibility requirements, interference to low voltage power line communication may sometimes be so strong that power line communication is

sometimes not working. According to [Li et al. 2008] this has prevented the use of power line communication in meter reading in China. But the same problem may be emerging also in Europe. Resolving this problem is needed. New modulation technologies may be less vulnerable to this problem, but experience with them is still needed.

Another major problem with Power Line Communication is the multitude of technologies, protocols, standards and proprietary solutions such as:

Open standards

    IEC 61334-5-1 S-FSK

    IEC 61334-5-2

    IEC61334-5-4

    CENELEC EN50090, ISO/IEC 14543 (KNX – PL)

    Echelon

    IEEE P1901

    ITU-T G.hn

    PRIME (not standardised)

G.hn is a next generation wired home networking standard developed by ITU-T, which supports high-speed communication over power lines, phone lines and coaxial cable.

Proprietary narrowband PLC technologies

    Telegestore–DLC

    ZIV Broadband PLC

    Homeplug

    Panasonic

    OPERA/UPA (DS2) , [OPERA], [UPA], [ekoplc 2008]

    ISTEON

Wired broadband DSL technologies

Digital Subscriber Line (DSL) means technologies for digital broadband (about 0.4–20 MB/s) data transmission over the wires of the telephone network customer connection. Typically the data rate to the service provider is lower and then the technology is also called Asymmetric Digital Subscriber Line (ADSL). 42% of the European homes had a broadband internet access connection in 2007 (Eurostat), predominantly provided as an ADSL connection through the existing telephone line and the penetration has been growing. ADSL shares the line with the voice service, but they operate at different frequencies separated by filtering and without disturbing each other. Data rates are far higher than those needed by smart metering. Lack of multicasting, service interruptions due to maintenance etc., lack of traffic prioritising and especially the lack of control by the metering operator mean that sharing with the consumers the normal low cost internet access based, for example, on ADSL services can cause serious unavailability problems for smart metering and related demand response services [ESMA 2010]. It is possible to separate and prioritize traffic via DSL by using ATM or Ethernet virtual LANs and prioritization. This is for example done for IPTV services. DSL as such provides the point-to-point service and it depends on the layers above like ATM, Ethernet or MPLS what kind of functions are supported and if prioritising traffic and dedicated access for the metering operator or the aggregator of distributed resources can be supported.

Plain old telephone service (POTS)

Plain old telephone service (POTS) is circuit switched and not packet switched. Thus it is relatively unsuitable for large scale smart metering and demand response applications, due to long connection times, relatively high costs, etc.

Other last km technologies that can be used in meter reading

The connection between users' meter-reading terminals and meter can also be based on some other wired or wireless technology. According to [Li et al. 2008] it can be a LAN, 485, CAN bus, HFC, telephone lines, power line etc; it can also be different radio technologies such as ZigBee (802.15.4) (or some other meshed radio network), Bluetooth, WiFi (802.11) or it can be Ethernet etc. In some areas there are Cable TV networks and optical access networks; sharing these for me-

tering and demand response often is subject to similar considerations as discussed above regarding the DSL.

5.3.5 Upgradeability of meters

To enable smart grids, it is essential to be able to upgrade firmware, such as meters, in the field without visiting the site for replacing the equipment or manually upgrading the firmware of the meter. Remote image download capability, common practice today in many embedded computing devices, will permit certain characteristics of the meter to be substantially altered on an as needed basis,[NIST 2010, p. 77]. As a response to the NIST Smart grids request NEMA developed the standard NEMA SG-AMI 1-2009 on the requirements for the upgradeability of smart meters. The standard is available from NEMA's Web site (www.nema.org) at no cost.

6. External interfaces of the metering operator

This chapter discusses the interfaces of the metering operator with other actors except for the interfaces with the homes and buildings which are dealt with in a separate Chapter 7. These interfaces provide metered data and load control services to the actors needing them. The actors were discussed in the Chapter 4 and include

- electricity market actors such as electricity retailers, aggregators of distributed energy resources and balance responsible parties

- system operators

- network operators that are the distribution network operators and the transmission system operator

- providers of energy analysis services for energy saving and energy trade

- authorities that control the efficiency of network operators and monitor the efficiency of energy end use.

In most countries including the Nordic countries billing metering is the responsibility of the distribution network operator and the transmission network operator is also the system operator.

Common standard interfaces are necessary for the data communication between the electricity market actors. The harmonisation between countries is still inadequate and needs to include a smooth transition from the traditional EDIEL and EDIgas messages to more modern, safe and secure ebXML protocols. Implementing and maintaining several data communication formats is rather expensive so the actors prefer to use the electricity market messages also for other purposes, when possible.

EDIEL and EDIgas

EDIEL and EDIgas are based on the UN EDIFACT standard. In the Nordic countries national interpretations of the EDIEL standard have been developed and are still used. But especially the international actors implement data exchange based on ebXML also in the Nordic Countries.

Compared to object oriented UML and XML based data formats the EDIEL and EDIgas are cryptic, inflexible and require specific software, and thus more difficult to apply for new purposes.

For balance settlement communication in Finland EDIEL is used with confirmation using APERAK. This covers normal situations, but the handling of exceptional situations and validation such as missing or erroneous data must be done before EDIEL communication. Status information is missing from EDIEL so only validated data should be sent. This leads to problems with hourly interval data.

ebXML

European Forum for Energy Business Information Exchange ebIX (www.ebix.org), European Transmission System Operators ENTSO E www.entsoe.eu), EFET (www.efet.org), and IEC TC57 WG 16 develop and standardise information exchange between energy market actors. Such information exchange includes also metered data. These are based on ebXML that was developed by UN/CEFACT and OASIS to replace EDI for electronic data exchange. ebXML is built on top of XML and Web services.

EFETnet

EFET is a federation consisting of the major European Energy Traders which defines standards for energy trading. EFETnet is a B2B (Business to Business) integration project based on EFET standards.

IEC 62325

There is also IEC Technical Committee 57, Workgroup 16, Electronic communications in deregulated energy markets and IEC 62325 is the corresponding standard.

TeMIX

OASIS Energy Market Information Exchange Technical Committee (eMIX TC) works to define standards for exchanging pricing information and product definitions in energy markets. It is open to all interested parties. It is developing an information model for energy transactions in the smart grid named Transactional Energy Market Information Exchange (TeMIX), see [Cazalet 2010]. The eMIX TC works closely with the OASIS Energy Interoperation TC, which develops Web services-based information and communication models for exchanging dynamic pricing, reliability, and emergency signals and information on energy market participation (such as bids), load predictability, and generation.

IEC CIM

IEC CIM is being extended to smart grid and demand response messaging. The central IEC CIM standards are IEC 61850, IEC 61970 and IEC 61968. They use TCP/IP communication, except for some time critical communication in IEC 61850. IEC-61850 is built on top of the Manufacturing Message Specification MMS (ISO 9506). Communication with field equipment is based on IEC 61850 and for back office applications the basis is IEC 61968. IEC 61968-9 standard is responsible for meter reading and meter control interfaces between systems. It is primarily intended for metering of electricity but it can be used to gas, water and heat metering as well. Typical uses of the message types include meter reading, meter control, meter events, customer data synchronization and customer switching.

Diverse

Customer information services may use MS Pitchtalk in communication. Data communication for power quality monitoring is at present non-standardised or based on substation automation protocols.

7. Interfaces of metering infrastructrures with homes and buildings

7.1 Applications and functionalities requiring AMI interfaces to home

Applications that need to exchange information with AMI include such as energy saving, demand response, embedded power generation, interfacing to energy markets, and power quality monitoring at the customer side. Also various leakage, health, safety, and security monitoring services may need interval data on consumption. In principle the time resolutions and time delays should be determined based on the relevant dynamics of the system in question. This kind of reasoning typically leads to 3–15 minute time intervals, when considering the building energy balances or the loadability of the electricity grid. For example, according to [Koponen et al. 2008] optimizing the energy use in buildings based on the building thermodynamics requires 5 minute or better measurement interval for energy consumption.

Energy saving and reducing CO_2 emissions need both

- real time consumption data for immediate feedback

- historic consumption data supported with expert analysis and performance comparison with peer group.

Here the real time means about 1 minute delay and time resolution. Building energy performance benchmarking is the basic and most important comparison service and may be implemented as software running in an internet portal, offered by a third party. This basic budget service can be supplemented by a more expensive expert analysis service.

Energy savings are best achieved by applying both

- manual actions based on both immediate and historic information from customer displays and

- home or building energy automation.

The objective is to reduce energy use and CO_2 emissions in the whole energy system. In the electricity system these depend very much on the timing of the consumption so focusing to energy end use reduction alone can sometimes lead to wrong actions such as removing such heat storages which, although locally increase some losses, help to reduce system level emissions by levelling out load peaks. Thus especially in the future electricity systems with much intermittent generation from renewables it is important that demand responds to the situation in the electricity market and grid.

Minute level immediate consumption feedback is also best for demand response and interfacing to the energy markets. The electricity market interface needs to be compatible with the time resolution and schedules of the markets participated such as the next day spot market, intra day energy market, and reserves and balancing markets. The value of the demand response is higher on the markets requiring faster response, but also the costs increase. For maximising the benefit and minimising the risks of market participation it is also important to predict the load, its responses and flexibilities accurately. This typically requires modelling the loads based on minute level (1–15 minutes depending on the case) interval measurements of the responses.

Consumption measurement time resolution better than one hour is required by many building energy automation and management functions such as peak power limitation and thermal dynamics based energy use optimisation, which both need 5 minute or better resolution for electricity consumption. That is why the Building Automation Forum in Finland (BAFF) and also a Finnish research project eCertification, when commenting the renewal of electricity market legislation in Finland, suggested that all new kWh-meters installed after a certain date should include a local interface for immediate consumption feedback. According to the new legislation customer gets a meter with such an interface, if he pays for the change of the meter. When there was no adequate common open standard for this interface, it was difficult to make this interface compulsory for every meter. What is required for at least 80 % of the measurement points of each DSO is measurement and settlement based on hourly interval data and access over the internet to hourly interval measurements next day for all the electricity market

actors. This includes the consumers and actors authorised by them. The need to use own current measurement instruments for immediate consumption feedback is an essential problem that has been discussed in building automation forums and the discussion continues [BAFF 2008].

Compulsory local interface for immediate information has been considered necessary and more than covering its costs from the point of view of the electricity end user or the whole society in many foreign and international cost benefit analyses and recommendations, such as [Crossley 2007, Kemp. et al. 2008, PCE 2009, ESMA 2010]. (The electricity customer is assumed to pay at the end all the costs, which seems to be a valid assumption regardless of the system, regulation, and legislation. If the scope of cost-benefit analysis is limited to the distribution network operator only, no form of smart metering was able to cover the costs of smart metering.) Lack of adequate open standards for this interface was identified as the main challenge and barrier regarding this interface.

The lack of open standard interfaces or any interfaces from the meter to the home network has lead to temporary solutions. One of these is optically reading the impulse led of the meter, which is also applied by the home automation systems. A major problem with all impulse reading systems (also SO-pulses on twisted pair) is that the size of the impulse must be changed on both sides simultaneously. When the meter operator updates the meter impulse size the results will be in error. Another increasingly popular approach is that the customers install their own current measurement instruments in series with the billing meter and typically show their results as energy; these are suitable only for purposes that tolerate the resulting very high inaccuracy. Responsibilities regarding the safety of the self made installations may also need consideration. For these reasons it would be better that an open standard HAN (Home Automation Network) interface is included in the common minimum requirements of the meter.

7.2 Standards for AMI – home interfaces

Home Area Networks and other local networks need to meet certain requirements in order to properly enable smart metering, energy saving, demand response and smart grid applications. The following requirements are typically mentioned:

- based on open standard interfaces

- supported by a reliable certification process that guarantees interoperability

- layered architecture (ISO/OSI 7-layer model) that enables use of multiple transport, media access and physical layer technologies with the same application layers and network management tools

- secure two way communication

- supports both direct load control and price control

- direct immediate access to nearly real time consumption data

- enables future applications and services that use metered data

- supports embedded generation and detailed end use metering

- supports multi-utility metering.

For example, see ZigBee Alliance and HomePlug Powerline Alliance Joint Smart Energy Profile Marketing Requirements Document.

At the moment a problem is that proprietary protocols are typically offered for the communication between the meter and the customer. Another problem is that too many protocols are applied. There are many candidates for the common open communication standard, but it seems very likely that several standards will be applied also in the future for communication between the meter and the customer's systems and appliances. The use of proprietary protocols and the number of alternative standards are expected to reduce rather much.

ZigBee Alliance (www.zigbee.org) and HomePlugPowerline Alliance (www.homeplug.org) now develop together their Smart Energy Profile. Use cases are taken from Utility AMI 2008 OpenHAN, Southern California Edison, Texas PUC, and ZigBee Alliance Smart Energy Profile 1.0.

Here a brief overview of communication technologies in local networks is given. Most of these communication technologies are discussed in more detail in Deliverable D2.1/ Part 1 of the Open Meter project [OPENmeter] and in [ESMA 2010].

The following communications technologies are found in local networks at the customers:

- Euridis bus (IEC 62056-31 standard) over twisted pair

- M-bus (Meter bus), (EN 13757 Series standards) over twisted pair or radio. It is not a network but a bus system developed for the remote reading of consumption meters (such as electricity, gas, and water). See http://www.m-bus.com .

- D-bus (Dialogue bus) for large facilities

- Ibus EIB (ABB)

- ModBus over serial line and ModBus/TCP over TCP/IP. See http://en.wikipedia.org/wiki/Modbus

- EIA-485 over twisted pair with standard or proprietary protocols

- Echelon LonWorks (ANSI/CEA-709.1; EN 14908; ISO/IEC 14908 Parts 1, 2, 3, and 4) works on powerline carrier, twisted pair, radio and IP-tunnelling. LONMARK organisation publishes open but LonWorks-specific application data models. Nevertheless LonWorks is often, and typically in metering systems, used with proprietary (non-open standards) application data models due to power line performance reasons.

- HomePlug over powerline comprising HomePlug AV (200 Mbps at 2–28 MHz), HomePlug 1.0 (14Mbps at 4.5–21 MHz) and HomePlug Command&Control (5 kbps, using different frequency bands in USA, Europe, and Asia due to compatibility with local frequency band allocation)

- CEBus (EIA-600), powerline (at 100–400 kHz), twisted pair, coax, infrared, RF, and fiber optics

- X-10 over powerline

- KNX (EN 50090, ISO/IEC 14543) over twisted pair, powerline, RF, infrared, Ethernet)

- Ethernet.

Power line communication is discussed in http://en.wikipedia.org/wiki/Power_ line_communication. Also several competing specifications are mentioned there including

- HomePlug Powerline Alliance

- Universal Powerline Association

- HD-PLC Alliance

- ITU-T G.hn (for broadband over power lines, phone lines, and coaxial cables).

[Yousuf et al. 2008] lists standards on Power Line Communication: IEEE P1675, IEEE P1775, IEEE P1901 draft, OPERA, POWERNET, UPA, CEPCA, ETSI PLT, and HomePlug Powerline Alliance Standards, and then gives an overview of the HomePlug Standards [UPA]. An overview of Power Line Communication Technologies is given in [Yousuf & El-Shafei 2007]. IEEE working group IEEE P1901 is developing the IEEE 1901 Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications". [Galli & Logvinov 2008] stresses the importance of stan-dardization in the PLC context and gives an overview of the activities of the IEEE P1901 working group.

The CENELEC standard EN 50065-1 "Signalling on low-voltage electrical in-stallations in the frequency range 3 kHz to 148.5 kHz" specifies four different frequency bands:

- A-band (3–95 kHz) for power companies

- B-band (95–125 kHz) for all applications

- C-band (125–140 kHz) for home network systems with a mandatory CSMA/CA access protocol

- D-band (140–148.5 kHz for alarm and security systems.

It also specifies the maximum output level as a function of frequency.

In North America and Asia the allocation of frequency bands is different. Thus a technology originating outside Europe may not meet the European re-quirements.

Appropriate for communication with the meters are also UHF low power radio technologies operating in the 433(Asia)/868(Europe)/915(US) MHz and 2.4 GHz license free ISM-bands. Both open standards and proprietary protocols exist, such as:

- ZigBee (Based on IEEE 802.15.4), mesh network, 2.4 GHz, this is the most potential RF protocol at the moment

- Wireless M-Bus (EN 13757-4)

- Z-Wave (proprietary), mesh network, in Europe 868.42MHz

- Bluetooth (IEEE 802.15.1), point-to-point, 2.4 GHz, frequency hopping

- Wavenis (proprietary), tree, star or mesh topology

- ISTEON (proprietary), mesh topology, 902–924 MHz

- Plextek Ultra Narrow Band (proprietary)

- Everblu (proprietary)

- DASH7 (ISO-18000-7), mesh topology, 433 MHz worldwide, ultra low power, range 2 km.

IEEE 802.15.4 WPAN (Wireless Personal Area Network) is the basis for such upper layer specifications as ZigBee, 6loWPAN, WirelessHART or MiWi. These specifications attempt to offer a complete networking solution by developing the upper layers that are not covered by the IEEE 802.15.4 standard. The WPAN as such supports star and point-to-point topologies.

WiFi/WLAN based on IEEE 802.11 operating in the 2.4 GHz or 5 GHz band is in some systems used for communication between the meter and the concentrator connected to WAN.

Also RFID-like (e.g. inductive 135 kHz or 13.56 MHz) readers limited to close proximity, inductive couplers with IEC 62056-31 EURIDIS, infrared communication and twisted pairs are applied in local meter reading.

It can be expected that in the future the same meter can communicate with several RF technologies. There are already smart meter communication modems available for smart meter manufacturers that can communicate with GPRS, ZigBee and wireless M-Bus.

7.3 Broadcasting control signals to homes

For fast and reliable broadcasting of control signals over wide areas both radio transmissions and power line communication technologies have been used for a long time. Now as the smart metering rollouts proceed many old power line broadcasting systems are being removed.

European Radio Ripple control system is presently used in Germany (129,1 kHz and 139 kHz) , Hungary (135,6 kHz), Czech Republic and Slovakia.

Deployment is planned in some other countries. In Germany it is used by electricity network operators RWE and E.ON for load control. It can also be used for customer tariff switching, broadcasting information to customers, and regional alarming. It is unidirectional so it cannot replace two way communication technologies but can complement them by providing fast broadcast of control commands and tariff changes. It operates on VLF bands so the data rate is rather limited. The range of a single transmitter typically covers a radius of 300–500 km. In UK the BBC radio transmission is used for broadcasting of load control signals.

8. Standards related to energy management at customer´s premises

8.1 Standards for different levels of home and building automation

The suitability of a particular protocol depends on the size of the automation system and the part of the automation system considered. Here protocols are presented in the order based on their suitability to different sizes of systems or different layers in the automation system hierarchy. First are the protocols most suitable for very small networks such as Home Automation Networks, next are protocols suitable for building automation at the field bus or local automation level, then protocols for the automation of very large buildings or groups of buildings, and last are protocols for communication between building control systems. The application areas of the particular protocols are overlapping so the order indicates the relative suitability compared to the other protocols. At the end, other potential solutions both wired and wireless are also listed. Finally, the most suitable PLC and wireless technologies are shortly discussed by the author.

This chapter is not an extensive list of existing standards. Instead, those communication protocol standards that the authors consider to be at the moment the most important for each segment are used as examples.

ZigBee is a proprietary wireless mesh networking standard that is optimised for low cost, low power consumption and low data throughput for Wireless Personal Area Networks (WPAN). The software is designed to be easy to develop on small, inexpensive microprocessors. ZigBee is used in local applications such as interconnecting sensors, home entertainment and control, energy monitoring and control. The Physical (PHY) and Medium Access Control (MAC) layers of ZigBee are defined by the IEEE 802.15.4 standard. ZigBee operates in the fol-

lowing radio bands that are available in different areas; 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz almost worldwide. ZigBee Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard. It develops application profiles the first being the ZigBee Home Automation profile. On March 3, 2009 the RF4CE (Radio Frequency for Consumer Electronics) Consortium agreed to work with the ZigBee Alliance to jointly deliver a standardized specification for radio frequency-based remote controls. On April 30, 2010 the ZigBee Alliance announced it has made the draft 0.7 document of ZigBee Smart Energy™ version 2.0 available for public download and comment, which is the Standard for Smart Metering and Energy Management in Home Area Networks. On May 24, 2010 the ZigBee Alliance announced collaboration with IPSO Alliance (www.ipso-alliance.org) on ZigBee IP and ZigBee Smart Energy 2.0. [ZigBee 2010]

HomePlug Powerline Alliance, Inc. is an industry-led initiative that creates specifications and certification logo programs for using the powerlines for reliable home networking and smart grid applications. The ZigBee and HomePlug alliances develop a common application layer for advanced metering infrastructure (AMI) and home area networks (HAN) that is called ZigBee smart energy profile. The HomePlug alliance has announced that it develops a compliance and interoperability program for products based on the IEEE 1901 Draft Standard. The aim is to ensure that many interoperable products will be available in the future. [HomePlug 2010]

KNX technology is an open, royalty-free and platform independent standard for home & building control. As KNX is based on more than 10 years of experience of its legacy systems (Batibus, EIB and EHS), it is a unique standard for Home and Building Control. KNX can be used to control various functions / applications in home and building, e.g. lighting, heating, ventilation, air-conditioning, blinds and shutters, monitoring, alarming, security systems, load management, etc. KNX can be installed in small-size single family dwellings as well as larger buildings. KNX is most suitable to be used in the field level. It is at its best in home automation solutions, not in large non-residential building automation solutions. It is approved internationally (ISO/IEC 14543-3, CENELEC EN 50090, CEN EN 13321-1, and Chinese Standard GB/Z 20965). Twisted pair (9.6 kbps, power line (1200 bps), RF (16 kbps), and IP are supported communication medias. [KNX 2010]

LonWorks is a standardized protocol applied for automation networks of buildings, energy management, metering and control, security systems, home automation etc. The LonWorks system is based on the LonWorks networking technology, which allows control devices from multiple vendors to communicate with one another through a common communication protocol that is shared among all devices. This technology allows intelligence and communications capabilities to be embedded into individual control devices that can be connected together through a variety of communications media. The common communication protocol is called LonTalk, and the embedded intelligence is provided by the neuron chip, an integrated circuit that combines the communications protocol, three microprocessors, a multitasking operating system, and an input/output scheme. The interoperability is based on Standard Network Variable Types maintained by LonMark International. This is necessary, because application specific technology independent protocols cannot be efficiently used with Lon-Works due to inadequate layering of the protocol. In smart metering systems proprietary application protocols are commonly used on LonWorks, because the relevant standard LonMark profiles are too inefficient on power line. LonWorks is most suitable to be used in the field level. LonWorks is at its best in certain home automation solutions, and also in non-residential building automation solutions. For relatively simple low cost home automation LonWorks is not as good as for example ZigBee or KNX. Due to cost issues, LonWorks has not been massively deployed in Europe, especially due to the existence of similar cheaper technologies, such as X-10. LonMark International has formed a partnership with EnOcean Alliance to provide a platform for bringing LonWorks protocol for wired and unwired networks together with EnOcean's RF end-device solution for low/no-power devices. [LonMark 2010]

BACnet is a standardised protocol for building automation and control networks. BACnet is suited to all kinds of building automation systems including HVAC, fire, and security systems. It consists of an object-orientated data model that represents the configuration and operation of a wide variety of operating and control devices. It also defines messages and services exchanged between devices on the client-server principle. BACnet supports all three hierarchical levels of building automation systems, though it is most suitable to be used in the automation and management levels. BACnet is at its best in large non-residential building automation solutions. The radio standard ZigBee and BACnet transmission based on Web services have been included in the standard; ANSI/ASHRAE

Standard 135–2008 defines the use of ZigBee as a BACnet data link layer. [BACnet 2010]

oBIX (for Open Building Information Exchange) is a standard for Web Services-based interfaces to building control systems [OASIS]. It is developed by OASIS the Organization for the Advancement of Structured Information Standards.

In this chapter the authors have described only those communication protocol standards that the authors consider to be at the moment the most important for each segment. In addition to KNX, other potential standard wired solutions include ITU G.hn, IEEE P1901, and PRIME. In addition to LonWorks and Home-Plug, other potential interfaces include proprietary technologies UPA [UPA], CEPCA [CEPCA], and X10. In addition to ZigBee, other potential wireless solutions include Wi-FI, Bluetooth, Wireless HART, and ISA100.

Considering the proper PLC technology to be used at the customer's premises, KNX, LonWorks, HomePlug C&C, and X10 also have license free operation in EU. KNX, LonWorks, and HomePlug could be solutions to smart metering and demand response applications. X10 is considered weak in meeting the reliability and data security requirements of these applications.

The most suitable wireless technologies to be used at the customer's premises include ZigBee IEEE 802.15.4 and Bluetooth in the low energy version (Blutooth-LE). The main advantages of IEEE 802.15.4 and Bluetooth LE are the following: frequency band available worldwide, very low energy consumption, low-cost and low latencies. Despite the bit rate of BT LE being larger, the bit rate provided by 802.15.4 is sufficient for the customer's premises. Another advantage of both technologies is that wide-spread interoperability with cell phones and laptops could be achieved in the next future. Either ZigBee or BT LE will be integrated into mobile phones in the next years. The main advantage of IEEE 802.15.4 with respect to Bluetooth, is the possibility to realise mesh and tree-based topologies. This means that with IEEE 802.15.4/ZigBee, scalable networks could be realised and the covered area could be very large. The authors consider ZigBee as the most promising technology for low cost wireless home automation networking. Other technologies that can be applied for this purpose were already mentioned in Chapter 7.

[Möllering & Löwenhag 2007] compared several communication technologies and standards for load control communication with smart appliances. Such communication could be coupled with AMR and its power line based or wireless access technology or be based on standardized plug&play home network tech-

nology. The technologies fulfilling the identified requirements and selected for final comparison were: power line technologies KNX and LonWorks, and wireless technologies WLAN/IEEE 802.11a-n, Z-Wave, ZigBee, and KNX RF.

For inclusion in the Smart Grid interoperability standards framework, release 1.0, standards for different applications were identified [NIST 1]. Related to interfacing AMI with the customer the following were mentioned: BACnet for building automation, Open HAN and ZigBee/HomePlug Smart Energy Profile for Home Area Network (HAN) device communication.

8.2 Standards for customer displays and Web Browsers

Standards for customer displays are given in W3C, CSS suggestions and recommendations. [Björkskog 2009]

9. Standards related to cyber security in metering infrastructures

Cyber security of smart metering infrastructures is becoming increasingly important, because of the following main reasons:

- Metering systems can provide a path for attacks against other connected systems.

- Metered detailed consumption data should not enter to unauthorised parties nor violate the privacy of the consumers.

- The authenticity and integrity of billing data must be guaranteed.

- In large scale the unavailability of control actions or wrong control actions may threaten even the security and safety of the electric power infrastructure.

There are several different standards or standard families that may be related to the cyber security in metering infrastructures. The reasons for this include:

- The holistic nature of security – it is very difficult or impossible to design the adequate security protection for the system, taking also into account all the potential threats of the future environment. These different security viewpoints are discussed in various specific standards.

- The variety of ICT technology alternatives that may be used in different interfaces of the metering infrastructure – the security solution and the related standard must fit to the selected system architecture and platform.

To begin from the high abstraction level, however, we want first to emphasize the importance of "defence-in-depth" principle.

9.1 Defence-in-depth principle

Layered defence for a metering system is built using

- several approaches to protection (such as host security, network security, application security, and also physical security)

- various security policies (such as electronic access policy, communication data filtering policy, data preservation policy, and cipher suite and cryptographic key negotiation policies)

- variety of feasible technologies (such as specific crypto techniques, secure protocol implementations, and system security management solutions)

- variety of security tools and procedures.

These and perhaps some other variant "layers" are needed to safeguard the whole system against various threats. The threats include, for example, any sudden disturbance in connected systems, internal and external attacks, effects of malware, theft, malicious access, and fraud. The standards related to defence-in-depth protection that can also be applied to metering infrastructure protection, include

- NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security

- U.S. Homeland Security, "Improving Industrial Control Systems Cyber security with Defence-In-Depth Strategies", October 2009.

9.2 Potential security standards for smart grids

In the U.S., the security considerations and feasibility analysis for smart grids have been started rather well. One of the best initiatives, the Cyber Security Coordination Task Group (CSCTG) organized by NIST, contributed promising results and involved more than 300 experts from both private and public sectors. The group continues today with the name Cyber Security Working Group (CSWG) http://www.nist.gov/smartgrid/ under the Smart Grid Interoperability Panel (SGIP).

Another good example of relevant standardization is UCAIug AMI-SEC Task Force http://osgug.ucaiug.org/utilisec/amisec/, which gives security guidelines, recommendations, and best practices for Advanced Metering Infrastructure sys-

tem elements. These specifications may be used to assess and procure the security functionality. Also, the vendors may develop compliant security solutions.

Recently we have been fortunate to see a specific report being available, namely [NISTIR 2010]. This report states that the following standards are directly relevant to the Smart Grid:

- NERC CIP 002-009, Cyber Security requirements for Critical Infrastructure Protection (CIP) by North American Electric Reliability Council. http://www.nerc.com/

- IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

- Security Profile for Advanced Metering Infrastructure, Advanced Security Acceleration Project – Smart Grid

- UtilityAMI Home Area Network System Requirements Specification

- IEC 62351, Parts 1–8, Information Security for Power System Control Operations (network & system security, TCP/IP & MMS profiles, ICCP & Sub-station protection).

The following listing of security standards is adapted from the same report, and we have tried to retain only the useful standards for smart metering, and also added few other standards.

Table 1. Security standards related to smart metering.

Organ-ization	Standard	Name	Working Group	Relevance
IEC	IEC 62351-1 (-8)	Data and Communications Security (for sub-stations)	IEC TC 57 WG15	Substation communication security
ANSI	ANSI C12.22	Meter and end device tables communications over any network	ANSI C12.22	Secure transport of metering data
DHS	DHS: Catalog of…	Catalog of Control Systems Security: Recommendations for Standards Developers	-	Management of security posture
IEEE	IEEE 802.11i	Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements	IEEE 802.11 WG	Wireless LAN security

9. Standards related to cyber security in metering infrastructures

IETF	SNMP	Simple Network Management Protocol	Network WG	Network management security
NERC	CIP 002-009	NERC Critical Infrastructure Protection (CIP standards)	NERC reliability	Requirements for management of system security
NIST	FIPS 140-2	Security Requirements for Cryptographic modules	Computer security	Crypto module security requirements
NIST	SP 800-82	Draft Guide to Industrial Control Systems (ICS) Security	Computer security	Security controls for ICS
UCAI-ug	UCAIug AMI-SEC	System Security Requirements	UCAIug	Security requirements for AMI elements
IEEE	802.1AE	Media Access Control Security Standard	IEEE 802.1 WG	MAC level security for LANs
IEEE	802.1X-2010	Port Based Network Access Control	IEEE 802.1 WG	Network access control for LANs
IETF	TLS	Transport Layer Security (TLS)	Network WG	Transport layer security protocol
IETF	DTLS	Datagram Transport Layer Security (DTLS)	Network WG	Transport layer security protocol
IETF	IPSec	Internet Protocol Security	Network WG	Network layer security, VPNs
IETF	SRTP	Secure Real-time Transport Protocol (SRTP)	Network WG	Secure transport of real-time data
IETF	SCTP	Stream Control Transmission Protocol (SCTP)	Network WG	Reliable message streams
IETF	Guidance for…	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management	Network WG	Guidance on AAA
NIST	FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)	Computer security	Data message integrity protection
NIST	FIPS 197	Advanced Encryption Standard (AES)	Computer security	Message confidentiality and integrity
NIST	FIPS 186-3	Digital Signature Standard (DSS)	Computer security	Authenticity of messages
NIST	PKCS #1, 3, 5, 12, 15	RSA Public Key Cryptography Standards	RSA Laboratories	Authentication, key agreement, encryption, message formats
ANSI/ INCITS	INCITS 359	Information Technology – Role Based Access Control	ANSI/INCITS	Access control

9.3 Cyber security of various technologies and protocols

In the following, we discuss the cyber security standards per communication technology or protocol, which can be used in the construction of the metering systems and related home and building automation functionalities. It should not be forgotten, however, that the security design should be based on system level risk analysis, incorporating a multifunctional team including various fields of expertise.

For in depth discussion of communication security in home and building automation, see [Granzer et al. 2009] and [Granzer 2010].

9.3.1 DLMS/COSEM security features

DLMS/COSEM has some feasible built-in security features that can be used to secure the data access and the data communications. Secure COSEM services are then transmitted by extended DLMS *application layer* protocol data units (PDU). The data units may be encrypted and/or authenticated, depending on the security policy in force at the communicating parties. The following details of DLMS/COSEM are according to [OPENmeter1].

Data access security

First, the authentication context is negotiated between the server and the client, which specifies the agreed authentication method and algorithm. One of three different security levels can be negotiated (No security, Low level security, High level security). The high level provides for the mutual authentication which is based on challenge/response based message exchange.

COSEM server can establish application associations (AA) with the clients which can have different roles and detailed (object, attribute, and method level) access rights (i.e. the role-based access control is supported). The application association is identified between the lower layer addresses of the end points of the connection.

Data transport security

In DLMS/COSEM, the cryptographic protection using ciphering may be applied to the data transport of PDUs. However, ACSE (Application Control Service Element) PDUs are not cryptographically protected by the services.

The security context is used to identify the relevant parameters that are used in the ciphering/deciphering process at the end-points. The security context consists of:

- Security policy (Not any / Authentication / Encryption / Auth+Encr)

- Security suite (AES-GCM-128 with AES-128 key wrap)

- Security material (ciphering & authentication keys, initialization vector)

- Structure of the ciphered application layer PDUs (security policy dependent).

9.3.2 DLMS/COSEM PRIME PLC security

In addition to DLMS/COSEM security features, PRIME PLC may use PRIME specific MAC layer secure connection and key management policy. This includes encryption, authentication and data integrity protection together with a negotiated security profile and a key management policy. All PRIME frames must be protected except REG and SEC control messages, and "Beacon" and "Promotion Need" PDUs.

The available security profiles are [OPENmeter1]:

- Security Profile 0: MAC SDUs without encryption

- Security Profile 1: AES 128-bit data & CRC encryption in ECB mode.

9.3.3 ANSI C12.22

ANSI C12.22 provides for application layer security, which is defined in the standard. The standard uses AES encryption and it is extensible for other security mechanisms and algorithms. It can be used for securely transporting the C12.19 metering data over different networks.

According to the ANSI C12.22 standard and [Moise & Brodkin 2009] the ANSI C12.22 application layer security mechanisms for messages are basically:

- AES-128/EAX authentication, integrity and encryption

- Replay protection.

However, a complete implementation of ANSI C12.22 security and authentication services, combined with the event logger of ANSI C12.19, includes:

- Encryption

- Authentication and integrity protection

- Credential management (ANSI C12.19)

- Intrusion detection

- Logging and auditing of all changes to data and configuration.

9.3.4 OMS – Open Metering System

The OMS specified security mechanism for wireless M-Bus link is:

- AES-128 encryption, authentication, and data integrity

- Replay protection (against fraud)

- Protection against traffic analysis (against monitoring user's presence)

    See [Evjen 2009] and [OMS 2009].

A key management scheme was also defined within OMS: Each meter is to be equipped with a unique cryptographic key only known to the utility. This key is transferred to the MUC when the meter is installed, over a secured TCP/IP link. After that, the AES secured data transmission may occur.

9.3.5 ZigBee (Field level)

The IEEE 802.15.4 (ZigBee belong to WPAN family of standards) security services include [Gascón 2009]:

- AES (32-128 bit) data encryption, frame authenticity and integrity protection

- Replay protection (counter)

- Access control based on received frame address.

The security modes that may be used with ZigBee:

- Unsecured (clear text data)

- Access Control List (list of authorized senders)

- Secured mode (encryption, message integrity, or both).

There is a support for secure link (point-to-point connection) between the two peers, and also secure group messaging using network broadcast key. The key management is organized by a dedicated coordinator node, which provides for device management, and the establishment and transport of cryptographic keys.

9.3.6 KNX (Field & Automation levels)

KNX/EIB does not provide any real information security features. There is only a simple access protection method (with 32-bit clear-text password) for limiting the unauthorized access to BCU (Bus Coupling Unit) services.

Due to limited computing resources of the field devices, the standard ICT security mechanisms cannot be used there. However, a unique security extension has been introduced, called EIBsec and proposed by [Granzer et al. 2006]. EIBsec introduces Advanced Coupler Unit (ACU) module which is added to each network segment that require secure communications. In EIBsec the secure communication is based on AES 128-bit encryption (Based on Secure Network Encryption Protocol (SNEP) and Secure EIB (SEIB) protocol). In EIBsec, two different encryption modes are available. The *normal mode* (only encryption) is used during session establishment and group key retrieval. The *counter mode* may be used for protecting management data (unicast) and process data (groups).

9.3.7 LonWorks (Field & Automation levels)

Unlike a device bus, LonWorks provides peer-to-peer communications. By avoiding the single "master" in the network, any LonWorks device may send data directly to another LonWorks device. As explained in http://www.rtaautomation.com/lonworks/ LonWorks provides a challenge-response mechanism for:

- Sender authentication and data integrity protection (64-bit MAC with 48-bit key)
- Replay protection (random number)
- Encryption not supported.

LonWorks protocol has serious security problems.

9.3.8 BACnet (Management & Automation levels)

By defining a number of discovery and data sharing services for automation devices and objects, BACnet protocol has rather multifaceted functionality including analog & digital IO, multi-state IO, file transfer, events, program, group data, etc. See: http://www.bacnet.org/. This functionality creates vulnerabilities, of course due to complexity, and also because BACnet can use various (insecure) data link protocols, such as BACnet over IP, ARCNET, Ethernet, LonTalk (part of LonWorks.), etc.

For security, BACnet provides only for old fashioned cryptography:

- Authentication, data confidentiality and data integrity with DES (not secure)
- Replay protection (random number).

The shared keys for DES are managed by a dedicated BACnet key server.

BACnet protocol has several security problems, so it should not be used without other security protocols for critical applications. (Also, in multiprotocol KNX/BACnet networks anyone needs to avoid single points of failure, e.g. gateways, hence each automation device could implement both BACnet and a KNX protocol stacks. Object database in application layer may then enable

BACnet vs. KNX data point mapping for the transmission.) See [Granzer et al. 2008]

9.3.9 Some IETF IP based protocols

If several different applications or data need to be secured between the devices, it often makes sense to apply a suitable VPN (Virtual Private Network) technology. VPN can protect the data communication interfaces from malicious attacks by dropping all inadequate data traffic, and also provides the secure tunneling for insecure protocols and data to traverse securely over various networks.

A useful information and comparison of various VPN protocols is available e.g. in NIST SP 800-77 "Guide to IPSec VPNs", Chapter 5.

TLS

How should the consumer securely access his/her private metering information that is collected by the DSO or the metering provider? The answer obviously is via the internet, most probably by using web browsing with HTTPS & TLS. The information provider has to generate a limited database view for this purpose, accessing only the relevant customer specific metering data.

Transport Layer Security (TLS) – IETF RFC5246 can cryptographically protect the information that the OSI transport layer 4 delivers. It can provide adequate security with:

- Payload data authentication, integrity verification and encryption

- Replay protection

- Public key certificate based mutual authentication of the peers.

The strength of the algorithms and key lengths are negotiated in the beginning of a secure TLS session, using a special handshake protocol. The handshakes can utilize public key certificates and cryptography (e.g. DSS, RSA) also for mutual authentication (server + client certificates), when necessary. The cryptographic key and policy negotiation messaging is rather well secured in TLS specification and most implementations. Also the strength of the strongest user data "Cipher-Suites" are very good (AES, 3DES, etc. are supported with long keys).

Also, the Datagram Transport Layer Security (DTLS) – IETF RFC4347 is a protocol that travels within the transport layer PDU. So, both TLS and DTLS

can traverse NATs and provide easy and secure device data exchanges without securing the transport layer or lower layers. This allows for example any client/server applications to communicate in straightforward way. DTLS over the Datagram Congestion Control Protocol (DCCP) – IETF RFC5238 is also one possible protocol to be considered.

IPSec

Security Architecture for the Internet Protocol – IPSec (IETF RFC4301-4309) is a family of protocols (of which AH and ESP are implemented at TCP/IP stack's network layer, or at least under transport layer). IPSec can provide adequate security in flexible ways using:

- IP header and payload data authentication, integrity verification and encryption (only ESP)

- Replay protection

- Public key certificate or shared secrets based mutual authentication of the peers.

The IPsec architecture consists of a number of specifications:

- Security Architecture for the Internet Protocol (IETF RFC4301)

- IP Authentication Header (AH) (IETF RFC4302)

- IP Encapsulating Security Payload (ESP) (IETF RFC4303)

- Internet Key Exchange (IKEv2) Protocol (IETF RFC4306)

- Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2) (IETF RFC4307)

- Cryptographic Suites for IPsec (IETF RFC4308)

- Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) (IETF RFC4309)

- Cryptographic Algorithm Implementation Requirements for ESP and AH (IETF RFC4835).

It should be noted that AH protocol cannot provide for encryption. On the other hand, there are two main modes available in which the ESP protocol (which can provide all the IPSec data security features) may operate:

- In the transport mode, ESP encrypts the transport layer and every bit of higher layers data.

- In the tunnel mode, ESP also protects the original IP header in addition to higher layers, and inserts everything inside an encapsulating IP (ESP) header.

The tunnel mode ESP (and IKE) are used in the construction of IPSec based Virtual Private Networks (VPNs). However, IKE is a rather resource consuming protocol for secure connection establishment with its complex ISAKMP message exchanges, but it is a scalable way to establish the secure connections between different parties of the infrastructure.

SNMPv3 protocol

In IETF there are two major choices for the management of IP devices:

- SNMP (ASN.1 encoded) system

- NetConf (XML encoded) system (not discussed here).

Simple Network Management Protocol (SNMP) is typically used over IP/UDP mostly for network management purposes to control any of the IP network attached devices. SNMP allows for a simple pull model-based implementation, which can be considered rather robust against various disturbances. Especially with SNMP version 3 (v3) developers can use various MIB (Management Information Base) views to the SNMP devices in secure ways. Different MIB views can be used e.g. to separate the network management from the meter data collection functions.

The User-based Security Model (USM), as defined in SNMPv3 (IETF RFC3414), provides for SNMPv3 security. It utilizes well-known algorithms to provide the security services. USM provides for:

- Authentication of a device/user

- Message encryption

- Data integrity checking

- Timeliness checking

- Etc.

SNMPv3 has the following security choices (levels):

- No security: Uses only clear-text username for authentication

- Authentication -level: Authentication based on HMAC-MD5 or HMAC-SHA

- Authentication & Encryption -level: Authentication based on HMAC-MD5 or HMAC-SHA. DES 56-bit encryption based on the CBC-DES.

SNMPv3 is defined in the following IETF RFC-documents:

- IETF RFC 3411 – RFC 3418

An alternative approach is to utilize even stronger, lower-layer security protocol to provide the security services for SNMP. For example, RFC5590 defines an extension which allows an "external" security protocol to be used with SNMP engines. Potential external protocols include TLS and SSH (RFC4251).

SCTP

A transport layer Stream Control Transmission Protocol (SCTP) – IETF RFC4960 is quite a recent, reliable protocol providing for independent message streams:

- May use TLS/SSL or run over IPsec

- Congestion avoidance behaviour

- Protection against flooding attacks (lightweight mutual authentication).

- Delivery mechanisms include:

    o Sequential non-duplicated delivery of messages for each independent stream

    o Immediate delivery (bypassing the sequential delivery).

SRTP

The Secure Real-time Transport Protocol (SRTP) – IETF RFC3711 defines a RTP (Real-time Transport Protocol) profile which provides for unicast and multicast RTP data security.

For encryption there are two cipher modes defined in SRTP which allow AES to be used as a stream cipher:

- Segmented Integer Counter Mode: AES with 128-bit key as default

- f8-mode: AES with 128-bit key as default.

Authentication, integrity and replay protection:

- HMAC-SHA1 as truncated to 80 or 32 bits size

- Hashing over the payload and the header including sequence number.

Cryptographic key establishment:

There are several possible choices that can be used for the negotiation and derivation of cryptographic keys that SRTP will need. Alternatives include:

- MIKEY (RFC3830: Multimedia Internet KEYing)

- SDES (RFC4568: Session Description Protocol (SDP) Security Descriptions for Media Streams)

- ZRTP (IETF Draft: Media Path Key Agreement for Secure RTP).

9.4 For further study

The following is left for future studies:

- Security standards of various wireless technologies that may be used in the construction of smart metering infrastructures and related demand response services.

- Better explanations about the limitations and descriptions for secure usage of various standards.

- Security architectures discussion.

10. Ongoing initiatives

10.1 Metering standardization projects and efforts

10.1.1 Mandate M/441

The European Commission has issued a mandate for the standardization of Smart Metering functionalities and communication for usage in Europe for electricity, gas, heat, and water applications (M/441 – Annex 1). The objective is interoperability of technologies and applications within a harmonised European Energy Market. The standardization process is mandated to the 3 European Standards' Organizations (ESO) CEN, CENELEC and ETSI. Their focus in this work is on interoperability at the metering system and local area network. For more information see [ESO 2009]. The 3 European Standards' Organizations set up a Smart Meters Coordination Group (SM-CG), which established a group on communication and another on additional functions. The standardisation activity in response to Mandate M/441 should be complete byt the end of 2011.

The deliverables of the Mandate M/441 are standards or technical documents. Standards are voluntary technical specifications and common technical rules for products or systems to be placed on the market. The mandate calls for the development of European standards which provide harmonised solutions within an interoperable framework. Where necessary this framework should be based on communications protocols within an open architecture, with a view to achieving full interoperability. It is not intended to extend the scope of this harmonization to back office systems although these have to be modified appropriately to accommodate smart metering.

10.1.2 OPENmeter project

OPENmeter project is included in the standardization mandate M/441 issued by the European Commission. http://www.openmeter.com/.

10.1.3 NIST smart grids interoperability standards development

In the U.S. the NIST (National Institute of Standards and Technology) is implementing its roadmap for development of smart grid interoperability standards [NIST 2010]. This includes several AMI and HAN related activities such as priority action plans for:

- standard meter data profiles (updating of ANSI C12.19)
- standards for energy usage information
- standard demand response signals
- guidelines for the use of IP Protocol Suite in the Smart Grid
- guidelines for the use of wireless communications
- energy storage interconnection guidelines
- interoperability standards to support plug-in electric vehicles

It also includes cyber security risk management framework and strategy.

10.1.4 IEC smart grids standards development

IEC has set up a Smart Grid Strategic Group (SG 3) which has developed a framework for IEC standardization to achieve interoperability of smart grid devices and systems. The NIST smart grids interoperability roadmap [NIST 2010] includes about 10 IEC standards and IEC has agreed to actively support identified and prioritized action fields.

In IEC standardisation work related to metering system interfaces includes:

- TC13 WG 14, Data exchange for meter reading, tariff and load control, develops the IEC 62056 standards
- TC 13 WG15, Electricity Metering, Payment System
- TC57 WG15 Data communication security, updates the IEC62351 standard.

10.1.5 IEEE Working Groups

Draft Standard IEEE P1901 is the power line technology driven by industry requirements. For example, the Inter System Protocol for coexistence with other technologies is mandatory for P1901, and many Smart Grid industry features are already designed into the standard. An approved standard is expected before the end of 2010.

IEEE P2030 works on Guidelines for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads   (http://grouper.ieee. org/groups/scc21/2030/2030_index.html)

10.1.6 ITU Smart Grid Focus Group

ITU has setup a Smart Grid Focus Group http://www.itu.int/ITU-T/focus groups/smart/ . The specific activities are still somehow open as the first meeting is in the middle of June 2010.

10.1.7 Utility AMI Working Group

Utility AMI Working Group operates under the open SG Subcommittee of the UCA international Users Group, www.osgug.org/UtilityAMI. See [UCA 2008].

10.2 AMI related development of home networking standards

ZigBee Alliance (www.zigbee.org) focuses on defining the network, security and application software layers, providing interoperability and conformance testing specifications and managing the evolution of the technology. Part of this is developing the ZigBee+HomePlug Smart Energy Profile further.

The ZigBee Alliance and the DLMS User Association are together defining a method to transport DLMS/COSEM messages through ZigBee networks.

ITU-T has a group working on home networking standard G.hn.

10.3 Extending utility communication standards to integration of distributed energy resources

Extensions for distributed energy resources and their aggregation are being developed to IEC CIM standards that define common information models for the application level.

11. Discussion

The electricity infrastructure is globally adopting common open interfacing and data communication standards that are well in line with the layering principles of the ISO/IEC 7498 Open Systems Interconnection reference model. Such standards include the IEC 61850 standards for automation and protection of power distribution and for communication with distributed energy resources and the Common Information Model (CIM) for distribution management (IEC 61968) and energy management in electricity infrastructure (IEC 61970). The situation regarding the standardization of metering systems is not as mature. Within the metering systems North America applies ANSI standards and Europe uses IEC 62056 standards. Even systems based on the same standard are not always truly interoperable due to vendor specific extensions and tuning. For the communication with the end customers such as consumers and their systems and appliances the situation is even worse. There is not yet a commonly accepted standard for interfacing meters with the Home Area Networks (HAN) home energy displays and building energy management and automation networks.

The costs of implementing and maintaining smart grids, demand response, energy saving and other such applications of smart metering will be too high without adequate and reasonable standardisation of the communication and application interfaces. Improving standardisation of interfaces is also necessary in order to manage data security vulnerabilities of demand response and smart grid applications. There are data security challenges to be solved especially, when building and home automation networks are used when controlling appliances and other loads in the buildings and homes.

There are now strong efforts to improve the standardisation situation such as the European Mandate M/441 and related OPENmeter project, NIST smart grids interoperability standards development, Utility AMI Working Group, and ZigBee Alliance.

One can observe that the established home and building automation protocols are in general not yet designed to meet adequately the communication security requirements stemming from the interconnections with smart metering systems and demand response. Reliable and correct control actions are even more important than confidentiality and integrity of metered data. Many of these communication security problems can be found in many smart metering systems and submetering, too. These challenges include:

- proprietary protocols and data security solutions that make it impossible to analyse the data security without reverse engineering and related unwanted legal consequences. Security by obscurity does not provide any protection against experienced attackers

- necessity to conversions between multiple protocols thus introducing additional points of vulnerabilities such as gateways

- inadequate layering of some protocols

- missing, inadequate or poorly designed data security mechanisms.

Solutions can be expected to develop because the awareness is increasing and there are other needs to solve the communication security problems in the home and building automation.

12. Summary

Now there are many activities related to standardisation regarding smart metering. It has been realised that the lack of common open standardised interfaces is one of the main barriers for successful and cost efficient development of smart metering and related applications such as demand response, energy saving and provision of information to the customer. Especially there are needs and activities to standardize the communication with the energy consumers and their systems. This report reviewed the situation in this field.

13. Acknowledgements

References

Literature referred in this report

ASHRAE 2010. American Society of Heating, Refrigerating and Air-Conditioning Engineers. www.ashrae.org

BACnet 2010. BACnet Interest Group Europe. http://www.big-eu.org

BAFF 2008. Building Automation Forum in Finland, seminar 2008.

Björkskog, C., Jacucci, G., Lorentin, B., Gamberini, L. Mobile Implementation of a Web 3D Carousel with Touch Input. Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services. Bonn, Germany. 2009. 4 p. http://www.energyawareness.eu/beaware/uploads/091001_bjoerkskog.pdf

Cazalet, E., G. 2010. Transactional Energy Market Information Exchange (TeMIX), An Information Model for Energy Transactions in the Smart Grid, White paper on behalf of the OASIS Energy Market Information Exchange Technical Committee, May 14 2010. 29 p. http://www.oasis-pen.org/committees/download.php/37819/Transactional%20Energy%20White%20Paper%20Draft%20010.pdf

CEN 2010. European Committee for Standardization, homepage. http://www.cen.eu/cenorm/homepage.htm

CENELEC 2010. CENELEC/TC205 Home and Building Electric Systems (HBES). http://www.cenelec.eu

CEPCA. Consumer Electronics Powerline Communication Alliance (CEPCA) www.cepca.org

Crossley, D. 2007. Advanced Metering For Energy Supply in Australia, Prepared for Total Environment Centre, Final revised version 17 July 2007, 98 s. www.efa.com.au

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the

electronic communications sector (Directive on privacy and electronic communi-
cations).

Directive 2002/91/EC of the European Parliament and of the Council of 16 December
2002 on the energy performance of buildings.

Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on
Measuring Instruments. Official Journal of the European Union. Volume 47, 30
April 2004.

Directive 2006/32/EC of the European Parliament and of the Council on energy enduse
efficiency and energy services and repealing Council Directive 93/76/EEC
http://eurex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:114:0064:0064
:EN:PDF

Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009
concerning common rules for the internal market in electricity and repealing Di-
rective 2003/54/EC, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:
2009:211:0055:0093:EN:PDF

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009
concerning common rules for the internal market in natural gas and repealing
Directive 2003/55/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?
uri=OJ:L:2009:211:0094:0136:en:PDF

EC 2007. Proposal for a regulation of the European Parliament and of the Council estab-
lishing an Agency for the Cooperation of Energy Regulators, Brussels,
19.9.2007, COM(2007) 530 final, 2007/0197 (COD).

ekoplc 2008. Universal Powerline Association (UPA) and OPERA Announce Joint
Agreement on Powerline Access Specification, Global Access Specification sub-
mitted to IEEE P1901. http://www.ekoplc.net/en/news/upa/index.htm

ERGEG 2007. Smart Metering with a Focus on Electricity Regulation, ERGEG Report
(E07-RMF-04-03), 31 October 2007, http://www.energyregulators.eu/portal
/page/portal/EER_HOME/EER_PUBLICATIONS/CEER_ERGEG_PAPERS/Cust
omers/2007/E07-RMF-04-03_SmartMetering_2007-10-31_0.pdf

ERGEG 2009. Status Review on Regulatory Aspects of Smart Metering (Electricity and
Gas) as of May 2009, Ref: E09-RMF-17-03, 19 October 2009, www.energy-
regulators.eu, 69 p.

ESMA 2010. European Smart Metering Guide, edition 2010. Available at www.esma-
home.eu.

ESO 2009. Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability M/441, Smart meters co-ordination group, draft report, Version 0.4 – 2009-09-18, 47 p.

Evjen 2009. Peder Martin Evjen, Open Metering System, Metering International, Issue 4, 2009, pp. 110–112.

Galli, S. & Logvinov, O. 2008. Recent Developments in the Standardization of Power Line Communications within the IEEE, Communications Magazine, IEEE, Volume 46, Issue 7, July 2008, pp. 64–71.

Gascón, D. 2009. Security in 802.15.4 and ZigBee networks 5 February 2009. http://www.sensor-networks.org/index.php?page=0903503549

Granzer, W., Neugschwandtner, G. and Kastner, W. 2006. EIBsec: A Security Extension to KNX/EIB. In Konnex Scientific Conference, November 2006.

Granzer, W., Kastner, W. and Reinisch, C. 2008. Gateway-free Integration of BACnet and KNX using Multi-Protocol Devices. In Proc. 6th IEEE International Conference on Industrial Informatics (INDIN '08), July 2008, pp. 973–978.

Granzer, W., Praus, F. and Kastner, W. 2009. Security in building automation systems. IEEE Transactions on Industrial Electronics, 56, 2009. 9 p.

Granzer, W. 2010. Secure Communication in Home and Building Automation Systems. PhD thesis, Vienna University of Technology, February 2010. 190 p.

HomePlug Powerline Alliance 2010. http://www.homeplug.org

ISO 2010. International Organization for Standardization. http://www.iso.org

ITU-T 2010. The United Nations agency for information and communication technology, Telecommunication Standardization Sector. www.itu.int/ITU-T.

KNX 2010. KNX Association. http://www.knx.org

Koponen, P., Pykälä, M.-L. & Sipilä, K. 2008. Needs and availability of AMR data in energy performance evaluation of buildings (In Finnish) Espoo 2008. VTT Tiedotteita, Research Notes 2438. 62 p. + app. 3 p. http://www.vtt.fi/inf/pdf/tiedotteet/2008/T2438.pdf

Li Li, Xiaoguang Hu, Jian Huang, Ketai He. 2008. Research on the architecture of Automatic Meter Reading in Next Generation Network, Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on, pp. 92–97.

LonMark 2010   LonMark International. http://www.lonmark.org

M/441 EN, Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability. European Commission, Brussels 12 March 2009.
http://www.openmeter.com/documents/m441en.pdf

Moise A. & Brodkin, J. 2009. ANSI C12.22, IEEE 1703 and MC1222 Transport Over IP, IETF Internet Draft, 16 November 2009. 22 p.

Möllering, C. & Löwenhag, J. 2007. Communication Containers for Smart Appliances. D3.2 (working paper) of WP3 from the Smart – A project. enervision GmbH 2007, 16 p.

Kemp, A., Whitfield, A., Quach, B., Hedynach, Y. & D'Souza, T. 2008. Cost Benefit Analysis of Smart Metering and Direct Load Control: Overview Report for Consultation, Report for the Ministerial Council on Energy Smart Meter Working Group, NERA Economic Consulting, Sydney NSW Australia, 29 February 2008. 212 p. www.mce.gov.au .

NIST 1. http://www.nist.gov/smartgrid/standards.html (as updated June 3, 2009)

NIST 2. http://collaborate.nist.gov/twiki-sggrid/bin/view/_SmartGridInterimRoadmap/InterimRoadmapWorkshop1

NIST 2010. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010, 145 p. http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf, http://www.nist.gov/ public_affairs/releases/smartgrid_011910.cfm

NISTIR 2010. DRAFT NISTIR 7628, Smart Grid Cyber Security Strategy and Requirements, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, February 2010, 310 p.
http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf

OASIS. Open Building Information eXchange (oBIX) http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=obix

OMS 2009. Open Metering System Specification, Volume 1, general Part, Issue 1.2.0 17 July 2009, 21 p.

OPEN meter project included in the standardization mandate M/441 issued by the European Commission. http://www.openmeter.com/

OPENmeter 1. OPENmeter project deliverable D3.1 Design of the overall system architecture, 8 February 2010, 83 p.

OPERA http://www.ist-opera.org/

PCE 2009. Smart electricity meters: How households and the environment can benefit, Parliamentary Commissioner for the Environment, New Zealand, June 2009, 46 p. www.pce.parliament.nz.

SD 2006. Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. Services Directive.

STOK. http://www.stok.fi/teknologia.html

Villa, F. 2007. Smart metering regulation: what´s going on in Italy. Metering Europe 2007, Vienna, 2−4 October 2007. 26 slides.

UCA 2008. OpenHANTask Force of the Utility AMI Working Group under the open SG Subcommittee of the UCA international Users Group: Utility AMI 2008 Home Area Network System Requirements Specification, http://www.utilityami.org/

UPA. http://www.upaplc.org/.

Yousuf, M.S., Rizvi, S.Z. & El-Shafei, M. 2008. Power Line Communications: An Overview – Part II, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 7–11 April 2008, pp. 1–6.

Yousuf, M.S. & El-Shafei, M. 2007. Power Line Communications: An Overview – Part I, Innovations in Information Technology, 2007. Innovations '07. 4th International Conference on 18–20 Nov. 2007, pp. 218–22.

ZigBee 2010. Zigbee Alliance and Home Plug Powerline Allaince liaison. Smart Energy Profile 2.0 Technical Requirements Document, ZigBee-105553, Draft 24 April 2010, 291 p.

Other literature

Badano, A. 2006. Standardisering inom AMR, Elforsk, December 22, 2006, 69 p.

Badano A. 2007., Next Generation AMM systems, Elforsk report 07:66, Elforsk, Sweden, December 2007, 82 p.

Bosquet, M.L. 2004. GridWise Standards Mapping Overview, GridWise, 65 p. http://www.gridwiseac.org/pdfs/gw_standards_mapping_p14587.pdf

CHESSS 2007. CEN's Horizontal European Service Standardization Strategy, Module 6 Billing & Metering,   http://www.chesss.eu/mod_detail.cfm?moduleId=6

ESMA project web site, www.esma-home.eu

Galli, S. 2009. Keynote 1. PHY LAYER and standardization. Power Line Communications and Its Applications. ISPLC 2009. IEEE International Symposium on March 29 2009–April 1 2009 Page(s): xii–xii.

ITRON. Standard Interfaces Will Spur Rapid Development of Smart Metering, http://www.metering-europe.com/Default/Itron_press_release_5763.aspx

Johnson, T. 2008. Pre-study – Nordic Standardization of AMR Systems, Elforsk rapport 08:34, February 2008, 28 p.

Metering and Billing Europe and Metering and Billing Scandinavia Conferences.

Trygg, P. 2003. ASP-palveluliiketoiminta sähköyhtiöiden toimintaympäristössä. (In Finnish) Diplomityö, Tampereen teknillinen yliopisto, Sähkövoimatekniikka.

Standards

ANSI C12.18   Protocol Specification for ANSI Type 2 Optical Port

ANSI C12.19-2008   Utility Industry End Device Data Tables

ANSI C12.21   Protocol Specification for Telephone Modem Communication

ANSI C12.22   Protocol Specification for Interfacing to Data Communication Networks

ANSI/ASHRAE 135-2008	BACnet – A Data Communication Protocol for Building Automation and Control Networks, Includes Amendments j, l, o ,r s, v, and Errata (2009)
CENELEC 2002	CENELEC, Uncovering the mysteries of standardization in Europe, Primer on Standards, 2002
EN 1434-3:2008	Heat Meters. Part 3: Data exchange and interfaces
EN 13757-2:2004	Communication systems for meters and remote reading of meters. Part 2: Physical and link layer
EN 13757-3:2004	Communication systems for meters and remote reading of meters – Part 3: Dedicated application layer (M-Bus)
EN 13757-4:2005	Communication systems for meters and remote reading of meters – Part 4: Wireless meter readout (Radio Meter reading for operation in the 868-870 MHz SRD band)
EN 13757-5:2008	Communication systems for meters and remote reading of meters. Part 5: Wireless relaying
EN 13757-6:2008	Communication systems for meters and remote reading of meters. Part 6: Local Bus
EN 13321 series	Open data communication in building automation, controls and building management
EN 50090 series	Home and Building Electronic Systems (HBES) – Open Communication Protocol
ETSI	European Telecommunications Standards Institute, http://docbox.etsi.org/Catalog/The_ETSI_Standards_Catalogue.html
HomePlug	HomePlugPowerline Alliance, www.homeplug.org
IEC/TR 60870-1-1 (1988-12)	Telecontrol equipment and systems. Part 1: General considerations. Section One: General principles
IEC 60870-1-2 (1989-11)	Telecontrol equipment and systems. Part 1: General considerations. Section Two: Guide for specifications
IEC/TR 60870-1-3 (1997-04)	Telecontrol equipment and systems – Part 1: General considerations – Section 3 Glossary

IEC/TR 60870-1-4 (1994-07)   Telecontrol equipment and systems – Part 1: General considerations – Section 4: Basic aspects of telecontrol data transmission and organization of standards IEC 870-5 and IEC 870-6

IEC 60870-2-1 (1995-12)   Telecontrol equipment and systems – Part 2: Operating conditions – Section 1: Power supply and electromagnetic compatibility

IEC 60870-2-2 (1996-08)   Telecontrol equipment and systems – Part 2: Operating conditions – Section 2: Environmental conditions (climatic, mechanical and other non electrical influences)

IEC 60870-3 (1989-05)   Telecontrol equipment and systems. Part 3: Interfaces (electrical characteristics)

IEC 60870-4 (1990-04) l   Telecontrol equipment and systems. Part 4: Performance requirements

IEC 60870-5-1 (1990-02) l   Telecontrol equipment and systems. Part 5: Transmission protocols – Section One: Transmission frame formats

IEC 60870-5-2 (1992-04)   Telecontrol equipment and systems – Part 5: Transmission protocols – Section 2: Link transmission procedures

IEC 60870-5-3 (1992-09) l   Telecontrol equipment and systems – Part 5: Transmission protocols – Section 3: General structure of application data

IEC 60870-5-4 (1993-08)   Telecontrol equipment and systems – Part 5: Transmission protocols – Section 4: Definition and coding of application information elements

IEC 60870-5-5 (1995-06)   Telecontrol equipment and systems – Part 5: Transmission protocols – Section 5: Basic application functions

IEC 60870-5-6 (2006-03)   Telecontrol equipment and systems – Part 5–6: Guidelines for conformance testing for the IEC 60870-5 companion standards

IEC 60870-5-101 (2003-02)   Telecontrol equipment and systems – Part 5–101: Transmission protocols – Companion standard for basic telecontrol tasks

IEC 60870-5-102 (1996-06)	Telecontrol equipment and systems – Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems
IEC 60870-5-103 (1997-12)	Telecontrol equipment and systems – Part 5–103: Transmission protocols – Companion standard for the informative interface of protection equipment
IEC 60870-5-104 (2006-06)	Telecontrol equipment and systems – Part 5–104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles
IEC/TS 60870-5-601 (2006-06)	Telecontrol equipment and systems – Part 5–601: Conformance test cases for the IEC 60870-5-101 companion standard
IEC/TS 60870-5-604 (2007-10)	Telecontrol equipment and systems – Part 5-604: Conformance test cases for the IEC 60870-5-104 companion standard
IEC 60870-5-SER (2007-10)	Telecontrol equipment and systems – Part 5: Transmission protocols – ALL PARTS
IEC/TR 60870-6-1 (1995-05)	Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 1: Application context and organization of standards
IEC 60870-6-2 (1995-10)	Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 2: Use of basic standards (OSI layers 1–4)
IEC 60870-6-501 (1995-12)	Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 501: TASE.1 Service definitions
IEC 60870-6-502 (1995-12)	Telecontrol equipment and systems – Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations – Section 502: TASE.1 Protocol definitions

IEC 60870-6-503 (2002-04)   Telecontrol equipment and systems – Part 6-503: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – TASE.2 Services and protocol

IEC/TS 60870-6-504 (1998-12)   Telecontrol equipment and systems – Part 6-504: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – TASE.1 User conventions

IEC/TR 60870-6-505 (2006-12)   Telecontrol equipment and systems – Part 6-505: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – TASE.2 User guide

IEC 60870-6-601 (1994-12)   Telecontrol equipment and systems – Part 6: Telecontrol
                               protocols compatible with ISO standards and ITU-T rec-
                               ommendations - Sect ion 601: Functional profile for pro-
                               viding the connection-oriented transport service in an end
                               system connected via permanent access to a packet
                               switched data network

IEC/TS 60870-6-602 (2001-04)   Telecontrol equipment and systems – Part 6-602: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – TASE transport profiles

IEC 60870-6-701 (1998-08)   Telecontrol equipment and systems – Part 6–701: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – Functional profile for providing the
                               TASE.1 application service in end systems

IEC 60870-6-702 (1998-10)   Telecontrol equipment and systems – Part 6–702: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – Functional profile for providing the
                               TASE.2 application service in end systems

IEC 60870-6-802 (2002-04)   Telecontrol equipment and systems – Part 6–802: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – TASE.2 Object models

IEC 60870-6-802 (2005-09)   Telecontrol equipment and systems – Part 6–802: Tele-
                               control protocols compatible with ISO standards and ITU-
                               T recommendations – TASE.2 Object models

IEC/TS 61085 (1992-04)   General considerations for telecommunication services
                               for electric power systems

IEC/TR 61334-1-1 (1995-11)   Distribution automation using distribution line carrier systems – Part 1: General considerations – Section 1: Distribution automation system architecture

IEC/TR 61334-1-2 (1997-12)   Distribution automation using distribution line carrier systems – Part 1–2: General considerations – Guide for specification

IEC/TR 61334-1-4 (1995-11)   Distribution automation using distribution line carrier systems – Part 1: General considerations – Section 4: Identification of data transmission parameters concerning medium and low-voltage distribution mains

IEC 61334-3-1 (1998-11)   Distribution automation using distribution line carrier systems – Part 3–1: Mains signalling requirements – Frequency bands and output levels

IEC 61334-3-21 (1996-03)   Distribution automation using distribution line carrier systems – Part 3: Mains signalling requirements – Section 21: MV phase-to-phase isolated capacitive coupling device

IEC 61334-3-22 (2001-01)   Distribution automation using distribution line carrier systems – Part 3–22: Mains signalling requirements – MV phase-to-earth and screen-to-earth intrusive coupling devices

IEC 61334-4-1 (1996-07)   Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 1: Reference model of the communication system

IEC 61334-4-32 (1996-09)   Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 32: Data link layer – Logical link control (LLC)

IEC 61334-4-33 (1998-07)   Distribution automation using distribution line carrier systems – Part 4–33: Data communication protocols – Data link layer – Connection oriented protocol

IEC 61334-4-41 (1996-08)   Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 41: Application protocol – Distribution line message specification

IEC 61334-4-42 (1996-10)	Distribution automation using distribution line carrier systems – Part 4: Data communication protocols – Section 42: Application protocols – Application layer
IEC 61334-4-61 (1998-07)	Distribution automation using distribution line carrier systems – Part 4–61: Data communication protocols – Network layer – Connectionless protocol
IEC 61334-4-511 (2000-04)	Distribution automation using distribution line carrier systems – Part 4–511: Data communication protocols – Systems management – CIASE protocol
IEC 61334-4-512 (2001-10)	Distribution automation using distribution line carrier systems – Part 4–512: Data communication protocols – System management using profile 61334-5-1 – Management Information Base (MIB)
IEC 61334-5-1 (2001-05)	Distribution automation using distribution line carrier systems – Part 5–1: Lower layer profiles – The spread frequency shift keying (S-FSK) profile
IEC/TS 61334-5-2 (1998-05)	Distribution automation using distribution line carrier systems – Part 5-2: Lower layer profiles – Frequency shift keying (FSK) profile
IEC/TS 61334-5-3 (2001-01)	Distribution automation using distribution line carrier systems – Part 5–3: Lower-layer profiles – Spread spectrum adaptive wideband (SS-AW) profile
IEC/TS 61334-5-4 (2001-06)	Distribution automation using distribution line carrier systems – Part 5–4: Lower layer profiles – Multi-carrier modulation (MCM) profile
IEC/TS 61334-5-5 (2001-09)	Distribution automation using distribution line carrier systems – Part 5–5: Lower layer profiles – Spread spectrum – fast frequency hopping (SS-FFH) profile
IEC 61334-6 (2000-06)	Distribution automation using distribution line carrier systems – Part 6: A-XDR encoding rule
IEC 61400-25	Communications for monitoring and control of wind power plants
IEC/TR 61850-1 (2003-04)	Communication networks and systems in substations – Part 1: Introduction and overview

IEC/TS 61850-2 (2003-08)	Communication networks and systems in substations – Part 2: Glossary
IEC 61850-3 (2002-01)	Communication networks and systems in substations – Part 3: General requirements
IEC 61850-4 (2002-01)	Communication networks and systems in substations – Part 4: System and project management
IEC 61850-5 (2003-07)	Communication networks and systems in substations – Part 5: Communication requirements for functions and device models
IEC 61850-6 (2004-03)	Communication networks and systems in substations – Part 6: Configuration description language for communication in electrical substations related to IEDs
IEC 61850-7-1 (2003-07)	Communication networks and systems in substations – Part 7–1: Basic communication structure for substation and feeder equipment – Principles and models
IEC 61850-7-2 (2003-05)	Communication networks and systems in substations – Part 7–2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)
IEC 61850-7-3 (2003-05)	Communication networks and systems in substations – Part 7–3: Basic communication structure for substation and feeder equipment – Common data classes
IEC 61850-7-4 (2003-05)	Communication networks and systems in substations – Part 7–4: Basic communication structure for substation and feeder equipment – Compatible logical node classes and data classes
IEC 61850-7-410 (2007-08)	Communication networks and systems for power utility automation – Part 7-410: Hydroelectric power plants – Communication for monitoring and control
IEC 61850-7-420 (2009-03)	Communication networks and systems for power utility automation – Part 7–420: Basic communication structure – Distributed energy resources logical nodes
IEC 61850-8-1 (2004-05)	Communication networks and systems in substations – Part 8–1: Specific Communication Service Mapping

	(SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3
IEC 61850-9-1 (2003-05)	Communication networks and systems in substations – Part 9–1: Specific Communication Service Mapping (SCSM) – Sampled values over serial unidirectional multidrop point to point link
IEC 61850-9-2 (2004-04)	Communication networks and systems in substations – Part 9–2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC 61850-10 (2005-05)	Communication networks and systems in substations – Part 10: Conformance testing
IEC/TS 61850-80-1 (2008-12)	Communication networks and systems for power utility automation – Part 80–1: Guideline to exchanging information from a CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104
IEC 61850-SER (2010-03-31)	Communication networks and systems in substations – ALL PARTS
IEC 61968-1 (2003-10)	Application integration at electric utilities – System interfaces for distribution management – Part 1: Interface architecture and general requirements
IEC/TS 61968-2 (2003-11)	Application integration at electric utilities – System interfaces for distribution management – Part 2: Glossary
IEC 61968-3 (2004-03)	Application integration at electric utilities – System interfaces for distribution management – Part 3: Interface for network operations
IEC 61968-4 (2007-07)	Application integration at electric utilities – System interfaces for distribution management – Part 4: Interfaces for records and asset management
IEC 61968-9 (2009-09)	Application integration at electric utilities – System interfaces for distribution management – Part 9: Interfaces for meter reading and control
IEC 61968-13 (2008-06)	Application integration at electric utilities – System interfaces for distribution management – Part 13: CIM RDF Model exchange format for distribution

IEC 61970-1 (2005-12)   Energy management system application program inter-
                               face (EMS-API) – Part 1: Guidelines and general re-
                               quirements

IEC/TS 61970-2 (2004-07)   Energy management system application program inter-
                               face (EMS-API) – Part 2: Glossary

IEC 61970-301 (2009-04)   Energy management system application program inter-
                               face (EMS-API) – Part 301: Common information model
                               (CIM) base

IEC/TS 61970-401 (2005-09)   Energy management system application program inter-
                               face (EMS-API) – Part 401: Component interface specifi-
                               cation (CIS) framework

IEC 61970-402 (2008-06)   Energy management system application program inter-
                               face (EMS-API) – Part 402: Common services

IEC 61970-403 (2008-06)   Energy management system application program inter-
                               face (EMS-API) – Part 403: Generic data access

IEC 61970-404 (2007-08)   Energy management system application program inter-
                               face (EMS-API) – Part 404: High Speed Data Access
                               (HSDA)

IEC 61970-405 (2007-08)   Energy management system application program inter-
                               face (EMS-API) – Part 405: Generic Eventing and Sub-
                               scription (GES)

IEC 61970-407 (2007-08)   Energy management system application program inter-
                               face (EMS-API) – Part 407: Time Series Data Access
                               (TSDA)

IEC 61970-453 (2008-06)   Energy management system application program inter-
                               face (EMS-API) – Part 453: CIM based graphics ex-
                               change

IEC 61970-501 (2006-03)   Energy management system application program inter-
                               face (EMS-API) – Part 501: Common Information Model
                               Resource Description Framework (CIM RDF) schema

IEC/TR 62051-1 (2004-01)   Electricity metering – Data exchange for meter reading,
                               tariff and load control – Glossary of terms – Part 1: Terms
                               related to data exchange with metering equipment using
                               DLMS/COSEM

IEC 62052-21 (2004-05)	Electricity metering equipment (a.c.) – General requirements, tests and test conditions – Part 21: Tariff and load control equipment
IEC 62054-21 (2004-05)	Electricity metering (a.c.) – Tariff and load control – Part 21: Particular requirements for time switches
IEC/TR 62055-21 (2005-08)	Electricity metering – Payment systems – Part 21: Framework for standardization
IEC 62055-31 (2005-09)	Electricity metering – Payment systems – Part 31: Particular requirements – Static payment meters for active energy (classes 1 and 2)
IEC 62055-41 (2007-05)	Electricity metering – Payment systems – Part 41: Standard transfer specification (STS) – Application layer protocol for one-way token carrier systems
IEC 62055-51 (2007-05)	Electricity metering – Payment systems – Part 52: Standard transfer specification (STS) – Physical layer protocol for a two-way virtual token carrier for direct local connection
IEC 62056-21 (2002-05)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange
IEC 62056-31 (1999-11)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 31: Use of local area networks on twisted pair with carrier signalling
IEC/TS 62056-41 (1998-11)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 41: Data exchange using wide area networks: Public switched telephone network (PSTN) with LINK+ protocol
IEC 62056-42 (2002-02)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 42: Physical layer services and procedures for connection-oriented asynchronous data exchange
IEC 62056-46 (2007-02)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol

IEC 62056-47 (2006-11)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 47: COSEM transport layers for IPv4 networks
IEC/TS 62056-52 (1998-11)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 52: Communication protocols management distribution line message specification (DLMS) server
IEC 62056-53 (2006-12)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 53: COSEM application layer
IEC 62056-61 (2006-11)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 61: Object identification system (OBIS)
IEC 62056-62 (2006-11)	Electricity metering – Data exchange for meter reading, tariff and load control – Part 62: Interface classes
IEC 62351	Power systems management and associated information exchange – Data and communications security.
IEC/TR 62210 (2003-05)	Power system control and associated communications – Data and communication security
IEC/TR 62325-101 (2005-02)	Framework for energy market communications – Part 101: General guidelines
IEC/TR 62325-102 (2005-02)	Framework for energy market communications – Part 102: Energy market model example
IEC/TR 62325–501 (2005–02)	Framework for energy market communications – Part 501: General guidelines for use of ebXML
IEC/TS 62325-502 (2005-02)	Framework for energy market communications – Part 502: Profile of ebXML
IEC/TS 62351-1 (2007-05)	Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues
IEC/TS 62351-2 (2008-08)	Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms

IEC/TS 62351-3 (2007-06)	Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP
IEC/TS 62351-4 (2007-06)	Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS
IEC/TS 62351-5 (2009-08)	Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives
IEC/TS 62351-6 (2007-06)	Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850
IEC/TR 62357 (2003-07)	Power system control and associated communications – Reference architecture for object models, services and protocols
IEEE 802.11-2007	IEEE Standard for Information technology -Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
IEEE 802.11k-2008	IEEE Standard for Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs
IEEE 802.11r-2008	IEEE Standard for information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific requirements part 11: wireless lan medium access control (mac) and physical layer (phy) specifications amendment 2: Fast basic service set (bss)
IEEE 802.11y-2008	IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Sys-

	tems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: 3650–3700 MHz Operation in USA
IEEE 802.11w-2009	IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames
IEEE 802.15.4-2006	IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).
IEEE 802.15.4a-d	IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendments to IEEE Std 802.15.4-2006.
IEEE 1547	IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems. IEEE, The Institute of Electrical and Electronics Engineering, 16 p.
IEEE 1547.1	IEEE Standard Conformance Test Procedures for Equipment Interconnecting Distributed Resources with Electric Power Systems
IEEE 1547.2	IEEE Application Guide for IEEE Std 1547™, IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems
IEEE 1547.3	IEEE Guide for Monitoring,Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems
IEEE 1675	IEEE Standard for Broadband over Power Line Hardware

IEEE P1775	Standard for Powerline Communication Equipment – Electromagnetic Compatibility (EMC) Requirements – Testing and Measurement Methods
IEEE P1901 draft	Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications
IEEE P2030	Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads
ISO/IEC 7498	Information technology – Open Systems Interconnection-Basic Reference Model
ISO 9506-1:2003	Industrial automation systems – Manufacturing Message Specification – Part 1: Service definition
ISO 9506-2:2003	Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol specification
ISO/IEC 14543-3-1:2006	Information technology – Home electronic system (HES) architecture – Part 3–1: Communication layers – Application layer for network based control of HES Class 1
ISO/IEC 14543-3-2:2006	Information technology – Home electronic system (HES) architecture – Part 3–2: Communication layers – Transport, network and general parts of data link layer for network based control of HES Class 1
ISO/IEC 14543-3-3:2007	Information technology – Home electronic system (HES) architecture – Part 3–3: User process for network based control of HES Class 1
ISO/IEC 14543-3-4:2007	Information technology – Home electronic system (HES) architecture – Part 3–4: Management procedures for network based control of HES Class 1
ISO/IEC 14543-3-5:2007	Information technology – Home electronic system (HES) architecture – Part 3–5: Media and media dependent layers – Power line for network based control of HES Class 1

ISO/IEC 14543-3-6:2007	Information technology – Home electronic system (HES) architecture – Part 3–6: Media and media dependent layers – Network based on HES Class 1, twisted pair
ISO/IEC 14543-3-7:2007	Information technology – Home electronic system (HES) architecture – Part 3–7: Media and media dependent layers – Radio frequency for network based control of HES Class 1
ISO/IEC 14543-3-3:2007	Information technology – Home electronic system (HES) architecture – Part 3–3: User process for network based control of HES Class 1
ISO/IEC 14908-1	Open Data Communication in Building Automation, Controls and Building Management – Control Network Protocol – Part 1: Protocol Stack. (EN14908-1)
ISO/IEC 14908-2	Open Data Communication in Building Automation, Controls and Building Management – Control Network Protocol – Part 2: Twisted Pair Communication. (EN14908-2)
ISO/IEC 14908-3	Open Data Communication in Building Automation, Controls and Building Management – Control Network Protocol – Part 3: Power Line Channel Specification. (EN14908-3)
ISO/IEC 14908-4	Open Data Communication in Building Automation, Controls and Building Management – Control Network Protocol – Part 4: IP Communication. (EN14908-4)
NEMA SG-AMI 1-2009	Requirements for Smart Meter Upgradeability
NTA 8130:2007	Netherlands Technical Agreement, Minimum set of functions for metering of electricity, gas and thermal energy for domestic customers. Netherlands Standardization Institute (NEN), August 2007, 25 p.

PLT ETSI PLT, http://www.etsi.org/website/homepage.aspx

W3C, CSS Transition Module Level 3, http://dev.w3.org/csswg/css3-transitions/, 2004

W3C, CSS3 module: Syntax, W3C Working Draft, http://www.w3.org/TR/css3-syntax/, 2003.

W3C, CSS 3D Transforms Module Level 3. http://dev.w3.org/csswg/css3-3d-transforms/, 2009

W3C, CSS Animations Module Level 3. http://dev.w3.org/csswg/css3-animations/, 2009

Author(s)
Pekka Koponen, Marja-Leena Pykälä, Janne Peltonen & Pasi Ahonen

Title

Interfaces of consumption metering infrastructures with the energy consumers
Review of Standards

Abstract

Standards for the data communication interfaces related to smart metering are reviewed in this report. The main focus is on the interfaces with the energy consumer's systems and appliances, but also the other interfaces are briefly discussed. Typically and increasingly these systems, meters and loads, such as appliances, are connected together via home automation or building automation networks. This interface is becoming increasingly important, because energy saving and demand response are needed more and more, and are enabled by the increase of intelligence in the electricity grids, houses and appliances. There are many protocols and standards, but the lack of a common open standard has delayed the development of the appliances and services that depend on these interfaces. This may also have delayed the development of functional and interface requirements for the meters. The problem has been widely detected and there are ongoing initiatives to solve it. Also these initiatives are briefly discussed. It can be observed that many protocols have significant shortcomings regarding data security. This problem is outstanding especially with the home and building automation protocols.

Tekijä(t)
Pekka Koponen, Marja-Leena Pykälä, Janne Peltonen & Pasi Ahonen

Nimeke

Energiankäyttäjien ja kulutusmittausjärjestelmien väliset tiedonsiirtorajapinnat

Katsaus standardeihin

Tiivistelmä

Tässä julkaisussa kartoitetaan energian kulutusmittausjärjestelmien tiedonsiirtorajapinto-jen standardeja. Pääpaino on rajapinnoissa energian loppukäyttäjien järjestelmiin ja lait-teisiin. Liitäntä tapahtuu yleensä ja enenevässä määrin rakennuksen tai kodin automaa-tioverkon kautta. Kyseisen liitännän merkitys on kasvamassa energiansäästön ja kysynnän jouston tarpeen sekä sähköverkkojen, talojen ja laitteiden älykkyyden lisääntyessä. Erilai-sia protokollia ja standardeja on monia, mutta yhteisen avoimen rajapintastandardin puute on hidastanut kyseisistä rajapinnoista riippuvien sovellusten ja palvelujen kehittymistä. Tämä on voinut hidastaa myös mittareiden toiminnallisten ja rajapintavaatimusten kehi-tystä. Ongelma on yleisesti havaittu ja käynnissä on hankkeita, jotka pyrkivät ratkaise-maan sen. Myös näistä hankkeista keskustellaan lyhyesti. Havaittiin myös, että tietoturvan toteuttamista vaikeuttavat siihen liittyvät puutteet monissa protokollissa. Erityisesti koti- ja rakennusautomaatioon liittyvässä tiedonsiirrossa tämä on huomattava ongelma.

VTT CREATES BUSINESS FROM TECHNOLOGY

Technology and market foresight • Strategic research • Product and service development • IPR and licensing
• Assessments, testing, inspection, certification • Technology and innovation management • Technology partnership

Standards for the data communication interfaces related to smart metering are reviewed. The main focus is on the interfaces with the energy consumer's systems and appliances, but also the other interfaces are briefly discussed. Typically and increasingly these systems and appliances are connected with the meter via home automation or building automation networks. This interface is becoming increasingly important together with the needs to save energy and increase demand response, enabled by the increase of intelligence in the electricity grids, houses and appliances. There are many protocols and standards, but the lack of a common open standard has delayed the development of the appliances and services that depend on these interfaces. This may also have delayed the development of functional and interface requirements for the meters. The problem has been widely detected and there are ongoing initiatives to solve it. Also these initiatives are briefly discussed. An observation was that many protocols have significant shortcomings regarding data security. This problem is outstanding especially with the home and building automation protocols.