Recent Advances in EN13757 Based Smart Grid Communication

Axel Sikora[1], Peter Lehmann[1], Naksit Anantalapochai[2], Martin Dold[2], David Rahusen[2], Alexander Rohleder[2]
[1] Laboratory Embedded Systems and Communication Electronics, University of Applied Sciences Offenburg, D77652 Offenburg, Germany
[2] Steinbeis Transfer Center Embedded Design and Networking, D79423 Heitersheim, Germany
Email: {axel.sikora, peter.lehmann}@hs-offenburg.de; {naksit.anantalapochai, martin.dold, david.rahusen, alexander.rohleder}@stzedn.de

Abstract—The communication technologies for automatic meter reading (smart metering) and for energy production, distribution and consumption networks (smart grid) have the potential to be one of the first really highly scaled cyber-physical applications. Due to the characteristics of the energy market, which is multi-“media”, multi-utility, and multi-vendor on the different levels of the value chain, standards are of key importance to guarantee interoperability and seamless communication. For the European markets, the EN13757 M-Bus standard family has become the standard of choice. However, the standard family is very flexible and can be adapted to the various requirements. This paper shall give an overview on the existing variants. The recent and actual advances are described in more detail. All information is backed by the experience from a fully independent implementation of the EN131757-4 of the authors’ team.

Index Terms—Smart grid communication, local metrological network, wireless M-Bus, EN13757

I. Introduction

Efficient, low-cost and stable communication solutions are a major stepping stone for smart metering and smart grid applications. This especially holds true for the so called primary communication or Local Metrological Network (LMN) between a local sensor or actuator and a data collector or gateway. LMNs have the potential to become the first cyber-physical applications with really large-scale multi-vendor installations, where small embedded sensors and actuators are interconnected to backend database services in the cloud.

M-Bus according to EN 13757 [1] is a major contender for LMN of Smart Metering and Smart Grid applications, as it holds the promise of a flexible, albeit optimized solution. It enjoys wide popularity in continental Europe, but increasingly in many other regions of the world. Especially, the Wireless M-Bus (EN13757-4) is characterized by a wide variety of different operation modes (C-, F-, N-, R2-, S-, and T-modes), which work in different frequencies (i.e. 868 MHz, 433 MHz, and 169 MHz).

Manuscript received April 28, 2014; revised September 16, 2014.
Corresponding author email: axel.sikora@hs-offenburg.de.
doi:10.12720/jcm.9.9.658-664

Although the basic EN13757-4 standard, which is presented in ch. II of this paper, already provides an enormous flexibility, various extensions and adaptations have been developed or still are under development. These additional dialects might have technical or non-technical background and add more complexity to a fundamentally relatively easy protocol. These dialects can be classified into three different groups, which are presented in more detail in the remainder of this contribution.

- The application layer (APL) may be adapted or restricted to certain use cases, as it is done by the activities of Open Metering System (OMS) Group [2], or Dutch Smart Metering Recommendations (DSMR) [3], also known as Netherlands Technical Agreements 8130 (NTA 8130) [4] commissioned by the Dutch Grid Companies (ENBIN). Also, other application layers can be directly integrated, like the “Device Language Message specification” (DLMS) and its “COmpanion Specification for Energy Metering” (COSEM) [5], [6]. These extensions are discussed in ch. III.
- The specifications of all layers may be adapted. This especially is the case for some country specific dialects, as specified from the Comitato Italiano Gaz (CIG) [7] in Italy or the Gaz réseau Distribution France (GRdF) [8] in France. These modified specifications are discussed in ch. IV.
- Extensions might also be derived along the requirements of security and privacy. The currently ongoing activities of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) can be seen as example for such security related extensions. The BSI has designed a Protection Profile (PP) and a Technical Directive (TR) for the communication unit of an intelligent measurement system (Smart Meter Gateway PP) [9] and for the Security Module of a Smart Metering System (Security Module PP) [10], which were first released in March 2013 and which partially refer to the secure LMN specifications of the OMS Group. They are presented in ch. V.

At the end of this contribution, various implementation related aspects and results are discussed in ch. VI.

II. The Basic EN13757

The different versions of M-Bus are specified by the European Standard EN 13757, which is worked out by TC294 at CEN/CENELEC. The EN 13757 is divided into the six parts from Table I. The M-Bus standard describes physical and data link layers as well as the application layer.

TABLE I: EN-13757 - COMMUNICATION SYSTEMS FOR METERS AND REMOTE READING OF METERS

Part	Title	Description
1	Data exchange	The first part describes the basic communication between the meters and a central data collector.
2	Physical and link layer	This part includes the specification of the physical data transmission using wired connections. It also includes the description of the protocol to transmit the data.
3	Dedicated application layer	The third part describes an application protocol, which allows the data transmission of meters multivendor capability. So devices of different manufacturers may be combined in one system.
4	Wireless meter readout	This part specifies the wireless communication of M-Bus and is its main document. It covers Physical and Data Link Layer and can be operated together with wired devices according to specification EN13757-2.
5	Relaying	The fifth part includes different proposals for routing the meter data to support larger distance between the meters and the data collector.
6	Local Bus	The last part contains a dedicated specification of a wired Physical Layer enabling lower cost for restricted cable lengths.

In these parts, EN-13757 describes different communication schemes (the so-called modes) for unidirectional and bidirectional data flow. These are described in Table II, which also shows the dazzling variety of options. The different modes allow an optimized fit to the different requirements of different markets, regions, and topologies.

Further information can be found at [12].

A. Frame Formats

Most of the Wireless M-Bus telegram information is composed of two main information blocks: the data link layer block and the application layer block. But in some cases, also an extended link layer, a transport layer or any higher layers block can be transmitted between the data link layer block and application layer block. Then, the blocks of these layers are also part of the telegram. Fig. 1 shows an example of a Wireless M-Bus telegram captured with the Wireless M-Bus capt³web sniffer [13].

The standard EN 13757-4 uses two different frame formats A and B (according to Fig.1, the telegram is in frame format type A). The frames are divided into blocks. In frame format type A the first block has a fixed length of 12 bytes containing the link layer block (10 byte address information plus two byte CRC). The second block starts with the Control Information field (CI-field) which is used to declare the structure of the following data and define the application protocol.

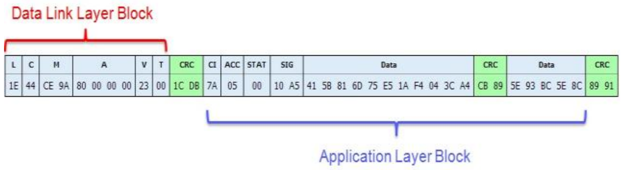

Fig. 1. Example of a wireless M-Bus telegram.

III. APL Related Extensions

A. OMS and DSMR

The basic EN13757 provides a very flexible and open specification, where some parts are not being described in detail or left reserved for future implementation. This left room and called for the activities of the OMS Group and DSMR.

OMS has restricted and defined the use of the fields in the wireless M-Bus telegram such as Control Field (C-field), Control Information Field (CI-field), Access Number Field (ACC-field) and also the data resolution in the application data block for the billing purposes. On the other side, DSMR has developed its specific extensions focusing on the application features and application data block.

An overview of the relations and differences between the standards is illustrated in Fig. 2.

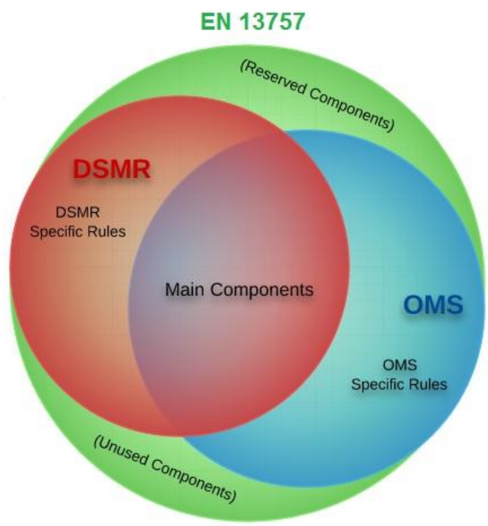

Fig. 2. Venn diagram showing the relation between standards [14].

It should be mentioned that both OMS and DSMR are available in different generations. The most recent versions in both cases are v 4. The history of the OMS versions is shown in Fig. 3. The most relevant DSMR versions are v 2.2 and v 4.

The protocol stack itself consists of three different layers: Application Layer, Data Link Layer, and Physical Layer, as it is shown in Fig. 4. A detailed description of the options and their interchangeability, as well as implementation issues are described in [14], where it is explained, how a consistent integrated solution can be provided.

TABLE II: OPERATING MODES OF WIRELESS M-BUS

mode		frequency	uni-/bi-directional	description
stationary	S1	868.3 MHz	unidir	The metering devices send their data several times per day. In this mode, the data collector may sleep most of the time. It must be woken up before the metering devices are sending data.
	S1-m	868.3 MHz		identical to S1, but the data collector must be constantly switched on
	S2	868.3 MHz	bidir	bidirectional version of S1.
frequent transmit	T1	868.95 MHz	unidir	The metering devices send their data at intervals of several seconds or minutes. suitable for walk-by and/or drive-by readout.
	T2	868.95 MHz 868.3 MHz	bidir	bidirectional version of T1.
frequent receive	R2	868.33 MHz 868.03 MHz + n*60kHz	bidir	by using frequency multiplexing several metering devices may be read simultaneously
	Q			protocol using precision timing
	P	868.33 MHz 868.03 MHz + n*60kHz	bidir	protocol using routers a network consists of one primary station (data collecting unit or concentrator) and a number of secondary stations. The network topology is hierarchical, with the primary station being the root node; secondary stations can act as router nodes, meter devices, or both. In order for the data collecting unit to establish the transmission path to any given network node in the tree, a search procedure and a network management protocol are defined which allow finding the nodes directly reachable and discovering the path to nodes not directly reachable.
compact	C1	868.95 MHz	unidir	similar to mode T but allows higher data rate with identical energy budget and duty cycle
	C2	868.95 MHz 869.525 MHz	bidir	The common support of mode T and C frames with a single receiver is possible.
narrow-band VHF	N1a-f N2a-f	169 MHz (@12.5 kHz)	unidir bidir	optimized for narrowband operation in the 169 MHz frequency band, which is a reserved band for meter reading and a few other services.
	N1g N2g	169 MHz (@50 kHz)	unidir bidir	sub-mode N2g mainly for long range secondary communication using multi-hop repeaters
frequent receive and transmit	F2	433.820 MHz	bidir	the bidirectional sub-mode F2 transmits a frame and waits for a short period for the reception of a response. This response will open a bidirectional communication channel.
	F2-m			wake up messages from a stationary or mobile transceiver to the meter device to open a communication channel.

Generation	Focal points	Status	OMS-specifications	OMS conformance test
1	Unidirectional wireless meters	withdrawn	Vol.1 issue 1.1.0 Vol.2 issue 1.0.2	-
2	Bidirectional wireless and M-Bus meters	Not recommended for new development!	Vol.1 issue 1.2.0 Vol.2 issue 2.0.0 Vol.3 issue 1.0.0	Version 1.1.0
3	Support of battery driven repeaters	Recommended for immediate certification	Vol.1 issue 1.4.0 Vol.2 issue 3.0.1 Vol.3 issue 2.0.0	Version 2.0.0
4	Security profile und conformity	Recommended for new development!	Vol.1 issue 2.?.? Vol.2 issue 4.0.2	-

Fig. 3. Overview of the OMS generations [2].

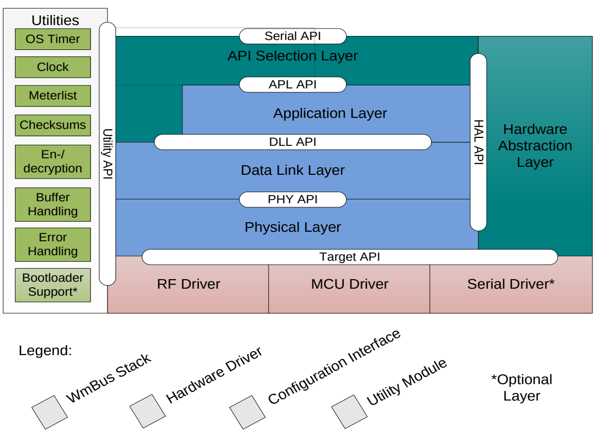

Fig. 4. Wireless M-Bus protocol stack architecture for flexible choice of application layers.

The tasks of the OMS group go beyond the specification of the application layer. Besides, security extensions are specified (task group security), a conformance test is prescribed and a test tool is being developed (working group 3). The specification of Wired M-Bus is under review to improve consistency (working group 4).

B. DLMS

Alternatively, it is also well possible to integrate a completely independent application layer. For a seamless end-to-end-communication between the end points (meter and backend server) without any application layer gateways in between, the "Device Language Message specification" (DLMS) and its "COmpanion Specification for Energy Metering" (COSEM) [5] are suitable candidates. All functions and use cases are specified by COSEM objects, the instantiations of COSEM interface classes (ICs). The data transfer is provided by the xDLMS application service element. The data collection application and the metering application are modeled as one or more application processes, APs. Therefore, in this environment communication takes place always between a client and a server AP: the client AP requests services and the server AP provides them.

This approach has been specified in a non-public deliverable of the EU-ARTEMIS-funded project "Smart Gas Meters & Middleware for Energy Efficient

Embedded Services” (ME GAS [15]). A similar approach is also used in the CIG approach (cf. ch. IV A).

IV. Country Specific Dialects

Europe would not be Europe without its national and regional specifics. In the case of Wireless M-Bus, this has led to two country specific dialects, which are described in the following. Both countries have a relatively monopolistic landscape of utilities.

A. *Italian CIG*

In Italy, the Comitato Italiano Gas (CIG [7]) has been working on a specification in fulfilment of the national UNI/TS 11291. After a period of around four years, it is publicly available since October 2013 [16].

The adaptations with regard to the lower layers are related to the following aspects:

- Broadcast messages
- Extra access to RF settings
- Dual stack capabilities
- ALOHA channel access
- LBT with exponential time backoff for unsolicited single channel access
- PM1 radio link management
- Minor changes at the PHY/RF settings with regard to the application layer, two important aspects must be regarded:
- Firmware download via broadcast and a maintenance window scheme
- An application layer derived from DLMS/COSEM.

B. *French GrDF*

In France, the Gaz réseau Distribution France (GRdF) [8] has worked on some extensions for the meter, the display and the LAN protocol [17]. The LAN protocol is mostly based on the prEN 13757-4 in its 2011 version with the following fundamental technological choices.

- Implementation of the N2 mode (bidirectional link over 169MHz bandwidth)
- Format of the manufacturer specific type of application grids
- Integration of advanced security functionalities

The protocol specification completes the original standard and specifies its implementation for the AMR channel as well as the required specific deviations and additions. These modifications mainly concern the following points:

- A generalization of the frequency channel management of the N-mode
- Optimized management of bi-directionality and transmissions sequencing
- A grid format that is adapted to the context of the GrDF application, very compact and maximizing the capacity of the radio channel and the autonomy of the metering devices
- A safer way to manage security (data coding, authentication of the transmitters, protection against denial of service, etc.)
- The definition of the broadcast mode for updating the metering devices
- The definition of a new experimental “high speed” modulation on a 12.5 kHz channel

V. Security Extensions

As applications in the smart grid are critical with regard to safety, security, and privacy, the German Federal Office for Information Security (BSI) was mandated by its governing ministry to design a Protection Profile (PP) and a Technical Directive (Technische Richtlinie – TR) for the communication unit of an intelligent measurement system (Smart Meter Gateway PP) [9] and for the Security Module of a Smart Metering System (Security Module PP) [10], which were first released in March 2013 and which partially refer to [11]. In Germany, these rules will be mandatory from 2015 onwards for newly installed meters with an annual turnover of more than 6 MWh or an installed energy producer with a peak power of more than 7 kW.

The *Local Metrological Network* (LMN) has to be secured – as all the other connection layers – with regard to both directions, i.e. from the meter to the SMGW and from the SMGW to the meter. I.e. an attack to the SMGW or to the meter devices shall be avoided.

Generally, a symmetrically encrypted link is required, where *Advanced Encryption Standard* (AES) will probably be the most widely used algorithm.

As the use of a static key allows cookbook attacks, a dynamic key exchange is required. This is provided by asymmetric cryptographic algorithms, so that the exchanged key can be applied by efficient symmetric cryptographic algorithms.

If a bidirectional communication is used, when parameter sets and/or even firmware versions are updated in the meter, then an additional mutual authentication is required. This can be performed together with the key exchange by asymmetric cryptographic algorithms. In addition, certificates can be used.

This set of functionality is used in the public internet since years and can be supported by the *Transport Layer Security* (TLS) protocol. Thus, it is reasonable to use that very protocol. To date, TLS is available in version 1.2, and has been significantly improved since its early *Secure Socket Layer* (SSL) days [18], [19]. In the normal LMN case, the gateway takes the role of TLS server, whereas the meter acts as TLS client. Both devices run a mutual authentication based on X.509 certificates and key exchange during the TLS connection setup.

It is clear that TLS poses high demands to the computing and the communication resources of the systems. For this reason, a session – using a single key – may be operated for a complete month (31 days), before a new session has to be established. As an alternative, the session has to be re-established after a data volume of 5 MBytes. During this period, session resumption is allowed, renegotiation is prohibited.

As TLS frames can come with a significant length, an additional *Authentication and Fragmentation Layer* (AFL) is defined for the mapping onto a lean, short frame data channel.

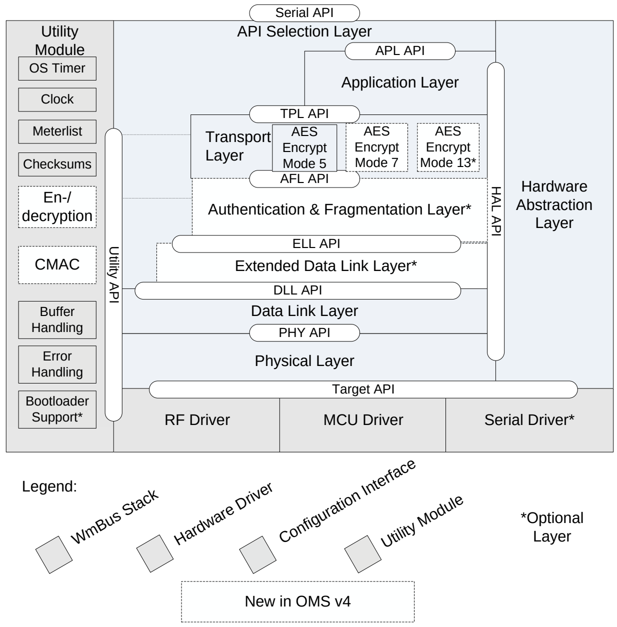

Fig. 5. Wireless M-Bus protocol stack architecture for flexible choice of application layers.

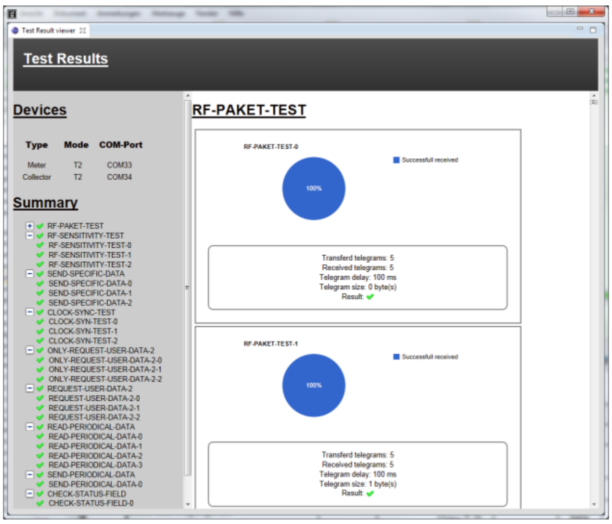

Fig. 6. Output of a successful test run.

In order to enable the integration of low-cost meters, the use of dynamic keys in symmetric cryptography is allowed, but its use is restricted to unidirectional communication from the meter to the SMGW, so that the meters cannot be tampered. Thus, the protocol stack sees a further extension, which is shown in Fig. 5. A detailed description of these specifications can be found at [20]

VI. Implementation Issues and Results

At the authors' team, an implementation of an extensible Wireless M-Bus protocol stack has been implemented, which supports in its current version many of the features being described above, i.e.

- Different modes (C-, N-, S-, T-modes);
- Various application layers (EN13757-3, OMS in different versions, DSMR in different versions)
- Parts of the security extensions.

A. *Modularity and Portability*

In addition to the functional flexibility a very high portability with regard to the hardware platforms, i.e. microcontroller and RF transceivers is enabled. This is realized by a strictly modular implementation concept based on layered software architecture to encapsulate the hardware related software modules (e.g. timers or persistent memory accesses) from the completely hardware independent Wireless M-Bus stack implementation.

In addition, the proper usage of preprocessor directives of the C language in combination with a software versioning system (GIT) allows configuration and optimization of the overall stack according to the applications' and/or customers' needs.

This approach helps to keep the code size at a reasonable level, as it is shown in Table III.

TABLE III: Code Sizes for Some Typical Stack Options on an ARM Cortex-M3 Microcontroller (EFM32LG990F256 with SI4461/SI4463)

Configuration	Read-only code memory	Read-write code memory	Read-only data memory	Read-write data memory
Collector C2	32204	288	760	4787
Collector T2	30264	288	720	4755
Collector S2	30088	288	468	4755
Collector N2	30196	288	732	4791
Meter C2	29300	288	472	4766
Meter T2	27660	288	472	4766
Meter S2	27492	288	432	4766
Meter N2	27748	288	696	4770

B. *Testing*

Especially before the background of the plethora of options, automated regression testing must be supported. This testing is performed on component level with the help of a PC-based commissioning and testing tool. A sample output of a test run is shown in Fig. 6.

In addition, the implementation is tested against third party products and the OMS conformance tester, as far as they are available.

C. *Simulation*

The stack can also easily be adapted for the evaluation in a network simulator. A more detailed description can be found at [21].

D. *Tools*

A Java-based fat-client has been developed for the parameterization of the nodes, for the visualization of properties (e.g. RSSI graph), for the commissioning of networks and network elements and also for the execution of the functional tests.

VII. Conclusions

The Wireless M-Bus protocol has evolved as a cornerstone of smart grid communication. This contribution shows the broad variety of extensions and demonstrates an implementation, which proves that high modularity, flexibility, and extensibility can be combined with a reasonable stack size, if – and only if – the rules of a stringent software engineering are followed.

REFERENCES

[1] Communication Systems for Meters and Remote Reading of Meters. European Committee of Standardization. 2011.

[2] Open Metering System Group. OMS Specification. [Online]. Available: http://oms-group.org/en/download4all/

[3] Dutch Smart Meter Requirements. Netbeheer Nederland. 2010. Main Document; Port 0, 1, 2, 3 and 4 Companion Standard.

[4] Minimum Set of Functions for Metering of Electricity, Gas and Thermal Energy for Domestic Customers. s.l.: Netherlands Technical Agreement (NTA 8130), 2007.

[5] DLMS UA 1000-1 Ed. 10.0:2010 COSEM Interface Classes and the OBIS Identification System, "Blue Book"

[6] DLMS UA 1000-2 Ed. 7.0:2009 DLMS/COSEM Architecture and Protocols, the "Green Book"

[7] S. Ghia, "Lo Stato di avanzamento della normativa tecnica," *Bologna*, vol. 11, April 2013.

[8] ENGLISH. [Online]. Available: http://www.grdf.fr/english

[9] Federal Office for Information Security. (March 2014). Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP). [Online]. Version 1.3. Available: https://www.bsi.bund.de/SharedDocs/……Zertifikate/PP/aktuell/ PP_0073.html

[10] Federal Office for Information Security. (March 2014). Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP). [Online]. Version 1.02. Available:https://www.bsi.bund.de/SharedDocs/……Zertifikate/ PP/aktuell/PP_0077.html

[11] Open Metering System, "Technical Report 01–Security," Issued 1.1.0, December 20, 2012.

[12] D. Lill and A. Sikora, "Wireless M-bus and its real-world flavors," in *Proc. Embedded World Conference*, Nuremberg, Germany, 2013.

[13] [Online]. Available: http://www.stzedn.de/capt2web-sniffer.html

[14] N. Anantalapochai and A. Sikora, "Development of a flexible application layer for wireless M-bus, OMS, and DSMR protocols," in *Proc. Embedded World Conference*, Nuremberg, Germany, 2014.

[15] A. Sikora and K. Landwehr, "Communication solutions for smart gas meters and energy efficient embedded services," in *Proc. Embedded World Conference*, Nuremberg, Feb. 29, 2012,

[16] UNI/TS 11291-1:2013. Sistemi di misurazione del gas - Dispositivi di misurazione del gas su base oraria – Parte 1: Caratteristiche generali del sistema di telegestione o telelettura. [Online]. Available: http://store.uni.com/magento-1.4.0.1/index.php/uni-ts-11291-1-2013.html

[17] GrDF, "Manual of gas distribution: Smart meters project - operational specification and detailed technique: LAN PROTOCOL," SINT000 Version 1.0, 28. Feb 2013.

[18] R. Oppliger, "SSL and TLS: Theory and practice," Artech House 2009.

[19] S. Jaeckel, N. Braun, and A. Sikora, "Design strategies for secure embedded networking," in *Long-Term and Dynamical Aspects of Information Security: Emerging Trends in Information and Communication Security*, A. U. Schmidt, M. Kreutzer, and R. Accorsi (Hrsg.), Eds., Nova Science Publisher, 2007.

[20] A. Sikora and M. Dold, "Architecture and development of secure communication solutions for smart grid applications," *Journal of Communications*, vol. 8, no. 8, pp. 490-497, August 2013.

[21] M. Schappacher and A. Sikora, "Network simulation of wireless M-bus networks," *Wireless Congress: Systems & Applications*, Munich, Germany, 2012.

Dr.-Ing. Axel Sikora holds a diploma of Electrical Engineering (M.Eng.) and a diploma of Business Administration (M.B.A.), both from Aachen Technical University. He has done a Ph.D. in Electrical Engineering at the Fraunhofer Institute of Micro-electronics Circuits and Systems, Duisburg, with a thesis on SOI-technologies.

After various positions in the telecommunications and semiconductor industry, he became a professor at the Baden-Wuerttemberg Cooperative State University Loerrach in 1999. In 2011, he joined Offenburg University of Applied Sciences, where he holds the professorship of Embedded Systems and Communication Electronics.

His major interest is in the system development of efficient, energy-aware, autonomous, secure, and value-added algorithms and protocols for wired and wireless embedded communication. He is founder and head of Steinbeis Transfer Center Embedded Design and Networking (www.stzedn.de).

Dr. Sikora is author, co-author, editor and co-editor of several textbooks and numerous papers in the field of embedded design and wireless and wired networking. Amongst many other duties, he serves as one of the four members of the Steering Board of Embedded World Conference, the world's largest conference on the topic.

Peter Lehmann holds a B.Eng. from Offenburg University of Applied Sciences. Since 2013, he is working as research engineer in the lab Embedded Systems and Communication Electronics of Offenburg University of Applied Sciences. His major interest is in the field of short range wireless networking, including 6LoWPAN and DLMS/COSEM.

Naksit Anantalapochai born in Brussels Belgium in 1988, graduated Bachelor of Computer Engineering from Faculty of Engineering, Chiang Mai University, Thailand in 2011. He finished his M.Sc. in the program "Communication and Media Engineering" from Offenburg University of Applied Science. He has a high interest in modern innovations and technologies especially in the field of embedded systems, communication networks and computer science. Since 2013, he is working in the Steinbeis Transfer Center Embedded Design and Networking on the application layers for Wireless M-Bus.

Martin Dold holds a B.Eng. in Information Technology of the Baden-Wuerttemberg Cooperative State University Loerrach. After having worked as lab engineer in the lab Embedded Systems and Communication Electronics of Offenburg University of Applied Sciences, he has joined Steinbeis Transfer Center Embedded Design and Networking for customer specific development of the Wireless M Bus stack.

David Rahusen holds a diploma (B.Eng.) in Electronical Engineering of the Baden-Wuerttemberg Cooperative State University Loerrach. After having worked as development engineer in Steinbeis Transfer Center Embedded Design and Networking, he led the development of communication products at with Conductix Wampfler. Since 2013, he is deputy head of Steinbeis Transfer Center Embedded Design and Networking and leads the development of Wireless M-Bus stack.

Alexander Rohleder holds a B.Eng. in Information Technology of the Baden-Wuerttemberg Cooperative State University Loerrach. Since 2010, he works with the Steinbeis Transfer Center Embedded Design and Networking in the core development of the Wireless M Bus stack.