Architecture and Development of Secure Communication Solutions for Smart Grid Applications

Axel Sikora
University of Applied Sciences Offenburg, D77652 Offenburg, Germany
Email: axel.sikora@hs-offenburg.de

Abstract—The communication technologies for automatic meter reading (smart metering) and for energy production and distribution networks (smart grid) have the potential to be one of the first really highly scaled machine-to-machine-(M2M)-applications. During the last years two very promising developments around the wireless part of smart grid communication were initialized, which possibly have an impact on the markets far beyond Europe and far beyond energy automation.
Besides the specifications of the Open Metering System (OMS) Group, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) has designed a protection profile (PP) and a technical directive (TR) for the communication unit of an intelligent measurement system (smart meter gateway), which were released in March 2013. This design uses state-of-the-art technologies and prescribes their implementation in real-life systems.
At first sight the expenditures for the prescribed solutions seem to be significant. But in the long run, this path is inevitable and comes with strategic advantages.

Index Terms—BSI protection profile, secure smart meter gateway, PKI

I. Introduction

Communication technologies are a major stepping stone for the upcoming application fields like smart metering and smart grid. They allow the timely observability and controllability of distributed elements in the generation, the distribution and the consumer networks. Due to the strong dependency, the robustness of a smart grid communication network against attack is of the utmost importance for the deployment of the smart grid [1] The security of these communication solutions is a central precondition for their successful application, as

- The functional safety of a system can be achieved only, if the security is guaranteed. This holds true both for the functional aspects of energy generation and consumption control as for the financial aspects of the smart energy market.
- Customers and companies alike will ask for privacy.

However, security is a significant challenge for smart meter networks, as

- A significant part of the communication paths will be wireless, so that there is no possibility for a physical protection of these paths.
- The local metrological networks (LMN) between the sensors (meters) and the data collectors (gateways) provide only limited capacity with regard to bandwidth and frame size.
- Many of the network elements are based on relatively small and low-cost embedded systems with only limited computing and memory resources.
- The systems envisage an extended time of operation. Even though individual elements, like meters, will be replaced after five to ten years, the overall communication architecture should be operated at least 15 to 20 years.

This contribution gives a short overview on the state of the art with regard to security approaches for smart grid communications (Section II), then presents the proposals of the smart meter gateway protection profile (Section III), and discusses some important implementation issues (Section IV). It shows a cost benefit analysis in Section V, before making some conclusion and outlook.

II. State of the Art

Worldwide, a lot of activities are ongoing to investigate on the solutions for secure smart grid operations. This includes

- A plethora of theoretical analyses and proposals, as they are summarized in excellent survey papers like [1] [2]or in the online bibliography [3],
- Generic standardization efforts like from the US-based NIST [4] or the Europe-based CEN-CENELEC-ETSI Smart Grid Coordination Group [5],
- Development of protocols and solutions for specific parts of the smart grid communication network, like IEC62351 [6]to be used over IEC61850, ZigBee Smart Energy Profile [7] or the specification from Wireless M-Bus EN13757 and Open Metering System (OMS) Group [8], [9].

In this charivari of activities, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) was mandated by its governing ministry to design a protection profile (PP) and a technical directive (TR) for the communication unit of an intelligent measurement system (smart meter gateway PP) [10] and for the security module of a smart metering

Manuscript received June 10, 2013; revised August,17 2013.
This work was supported in part by a grant from German Federal Ministry of Economy and Technology (BMWi) ZIM KF2471305ED2.
Corresponding author email: axel.sikora@hs-offenburg.de.
doi:10.12720/jcm.8.8.490-496

system (security module PP) [11], which were released in March 2013. 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.

These specifications attracted broad attention in the community, and are candidates for wide application far beyond Germany, and far beyond the single application of smart metering. Therefore, this contribution presents the major characteristics of these specifications.

III. BSI Smart Meter Gateway

A. Network Architecture

The technical directive consists of various documents on the different aspects of the overall architecture (cf. Fig. 1). These include the directives for the smart meter gateway (SMGW, BSI TR-03109-1), for the security module (BSI TR-03109-2), for the underlying cryptographic algorithms and implementations (BSI TR-03109-3), for the public key infrastructure (PKI, BSI TR-03109-4), and for the communication adaptors (BSI TR-03109-5). For the specific elements, additional test specifications are provided, so that a certification process can be supported.

Fig. 2 shows the different elements of the BSI network architecture, which includes

- The primary communication (*local metrological network, LMN*) between the local meter and the secure smart meter gateway (SMGW),
- The secondary communication (*home area network, HAN*), which allows the local monitoring of data and control of controllable local systems (CLS), like photovoltaic systems, combined heat and power (CHP) units, or alike,
- The tertiary communication (*wide area network, WAN*) between the SMGW, the provider of the functionality (utility) and additional administration personnel.

B. Positioning

The result of the PP comes with a certain model character, as

- The result of the specification is a reasonable compromise in a complex conflict of objectives. The achieved security level is ambitious, however, still realistic in terms of cost and administration complexity. It should be highlighted that – despite the quite specific requirements from the application – the specification is based on open and well established standards from the IT-world (i.e. like Transport Layer Security, TLS, like Common Criteria (CC) Certification), In order to make these rules applicable, a good number of specific implementation rules and guidelines are given.

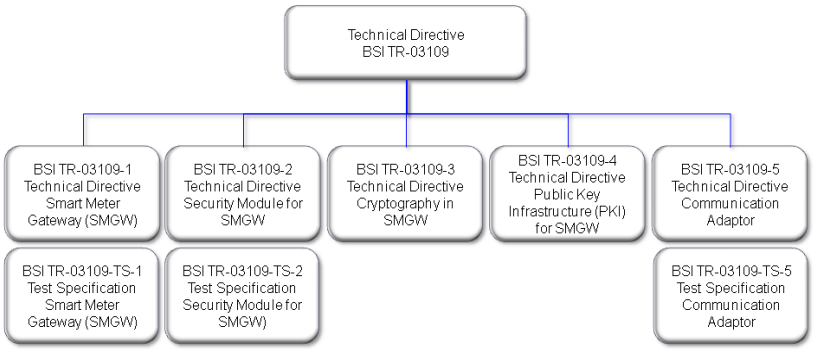

Figure 1. Secure smart meter gateway–overall structure of technical directive BSI TR-03109

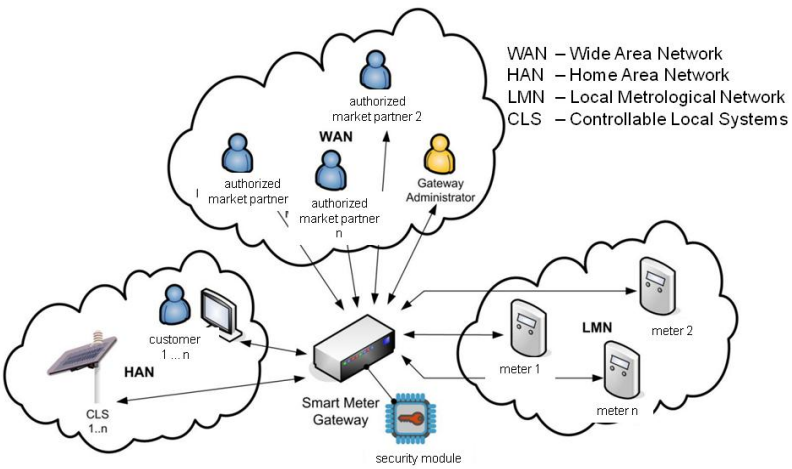

Figure 2. Secure smart meter gateway – overall communication architecture of secure smart grid infrastructure [10].

- The process of the specification is a good example for a guiding government, which regards strategic and customers interests, but also considers the interest of industry. The discussions were held in open discussions and extensive commenting rounds together with industry associations.

It should be mentioned that the result of the process, of course, also has some weaknesses, but it is important that the strategic setup is reasonable and future proof.

C. Securing the Local Metrological Network

The LMS 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. That is, 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 for the bidirectional use cases. This is provided by asymmetric cryptographic algorithms, so that the exchanged key can be applied by efficient symmetric cryptographic algorithms.

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 significantly improved since its early secure socket layer (SSL) days [12], [13]. 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. This can be performed together with the key exchange by asymmetric cryptographic algorithms. In addition, certificates can be used.

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.

In order to enable the integration of low-cost meters, the use of static 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. In doing so, it is assumed that the SMGW has some ex-ante knowledge about the meters in the field and can support some monitoring functionality, e.g. intrusion detection systems (IDS), intrusion prevention systems (IPS) and packet filtering (firewall). In the unidirectional, as in the bidirectional case – requires a mutual authentication, which is also realized in the AFL.

A write access to the metering unit is allowed after a mutual authentication, where the gateway has to authenticate against the metering unit. And even then, those parts of the metering unit being covered by standard weights and measures law are not to be accessed. As a rule, the SMGW is the only communication interface for meters in the LMN.

D. Securing the Wide Area Network

It is also required to secure the communication into the wide area network (WAN) by TLS, supporting version 1.2 as a minimum. A fallback to an older version is prohibited. For the WAN communication, the gateway takes the role of the TLS client, its counterpart in the WAN acts as TLS server. The connection setup starts with a certificate based mutual authentication, where the certificates are generated by the Smart Metering Public Key Infrastructure (PKI).

It is important to mention that the SMGW does not accept any incoming TLS connection requests from the WAN. But as it is essential to have arbitrary access to the gateway for administration and readout purposes, an additional wake-up service is supported. In case of a wakeup signal, the gateway connects to a pre-configured (and therefore secure) server in the WAN.

In case of WAN connection, the TLS session may be operated a maximum of two days. Also here, session resumption is allowed.

It is very important to have an extensive role concept for the users from the WAN. Most important roles are e.g. consumer, (energy) network utility, producer, and administrator. It is especially to be mentioned that

- It is assumed that the gateway administrator and the service technician are trustworthy and well-trained.
- The introduction of the role of external administrator is a very important towards a more flexible mode of system integration. In the end, it is clear that the role and the task of this administrator are not yet exactly and completely clarified. The tasks might include configuration, monitoring, administration of certificates and certificate updates, or NTP-server management.

Open questions in this context are mostly around the open issues of public Internet protocol family, like network time protocol (NTP) or domain name service (DNS) protocol, which possibly should be secured by their counterparts SNTP or SDNS.

E. Securing the Home Area Network

The local access has bug functional importance, as it allows the direct access to data and to devices. In conjunction with smart grid applications, the so called home area network (HAN) might also enable the connection of controllable local systems (CLS), i.e. decentralized generator units, like photovoltaic systems, combined heat and power (CHP) units, electric vehicle, or alike. These units can be remotely controlled by a backend system, where

the SMGW offers a TLS proxy service. There are two TLS connections being terminated in the SMGW: one connection from the backend to the SMGW, and one connection from the SMGW to the CLS.

If devices in the HAN have a separate connection to parties in the WAN (beside the gateway) this connection shall be appropriately protected, which in effect leads to

F. Securing the Gateway

Obviously, the SMGW plays a central role in the architecture, as it has to deal with the administration of the connections, with the encryption and decryption functionality, and with the storage of the key and certification materials. If the SMGW fails to be secure, then the complete security concept is to be questioned. Thus, it has to be especially secured and a security module has to be used. A security module is a secure cryptoprocessor that can store cryptographic keys and protects information. It might be a separate IC or a function block integrated into a CPU chip. A specification for such a trusted platform module (TPM) is developed by trusted computing group (TCG) [14]. In addition, BSI specifies a certified module along the rules of common criteria (CC).

The TPM secures the cryptographic identity of the gateway and offers cryptographic functions as a service provider. I.e. it enables functions for key generation, for generation and verification of digital signatures, and for key negotiation. In addition, it reliably generates random numbers, and securely stores keys and certificates.

The implementation of the complete SMGW shall conform to the evaluation assurance level (EAL) 4+ of Common Criteria. This EAL poses already high requirements with regard to the organization and the structure of the development processes.

It is assumed that the SMGW is installed in a non-public environment within the premises of the consumer which provides a basic level of physical protection. This protection covers the gateway, the meter(s) that the gateway communicates with and the communication channel between the SMGW and its security module.

The security module should be physically integrated into the SMGW, which includes sealing on the SMGW PCB. The mounting of the security module shall be done during the production process under secured conditions.

G. Logging

The SMGW shall also provide logging functionalities. This includes consumer logs, system logs and calibration logs. Different timing and access conditions apply.

IV. Implementation Issues

A. Overview

With regard to device architecture, two aspects are to be considered and currently being discussed. Both aspects mainly apply to the gateway and include the hardware architecture (cf. section B) and the software architecture (cf. section A).

B. HW Architecture

The BSI Protection Profile does not want to imply any concrete HW architecture for the components. However, it shows three examples of physical representations for the different components of the Smart Metering System – focusing on the SMGW.

Fig. 3 shows implementation type 1, where the SMGW is integrated into one device comprising [10]:

- The security relevant parts (i.e. SMGW security functionality, TSF)
- The non-security relevant parts of the SMGW, e.g. the unit for communication, and
- The Security Module that is a target of a separate evaluation but is physically located in the device.

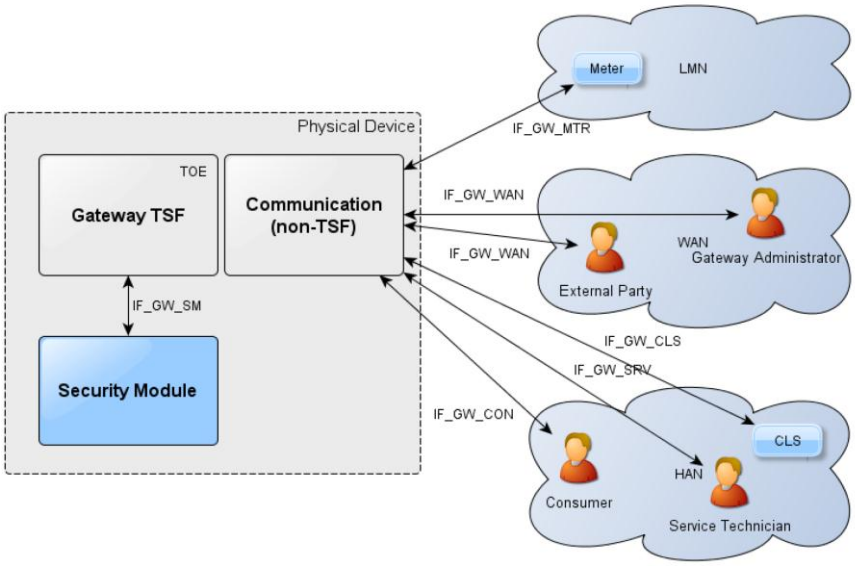

Figure 3. Architecture type 1 in one single device: a gateway and multiple meters; the abbreviation TSF stands for target of evaluation (TOE) security functionality) [10].

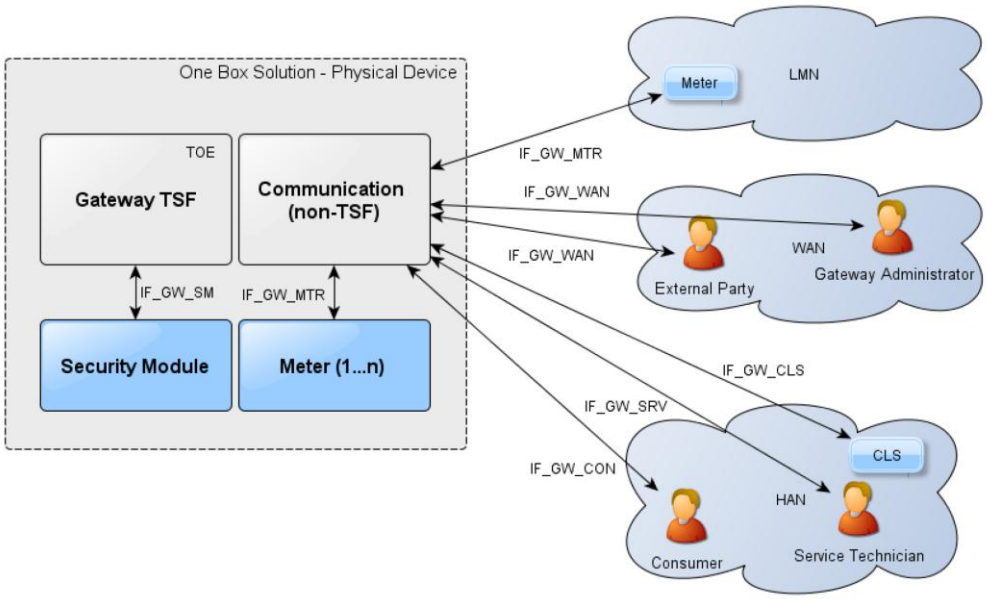

Figure 4. Architecture type 2 as a one box solution integrating gateway and Meter [10].

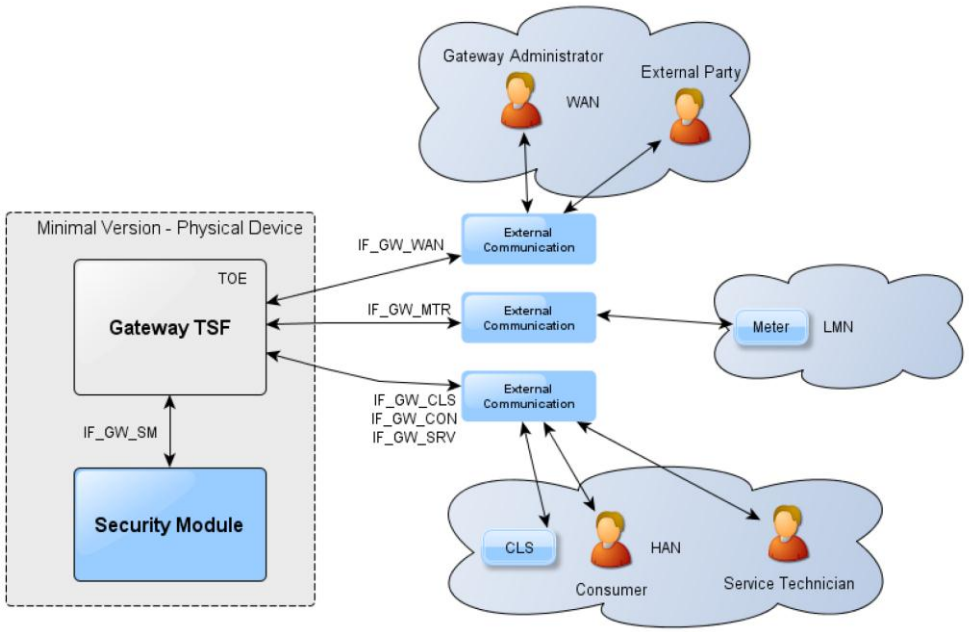

Figure 5. Architecture type 3: minimal implementation [10].

The Gateway communicates with one or more meters in the LMN, provides an interface to the WAN and provides interfaces to the HAN.

The components SMGW and meter might also be realized by a single physical device providing functionality of both. Such a “One Box Solution” is shown as type 2 architecture in Fig. 4. This solution may be the preferred implementation for one family houses or large houses with several flats where all electricity meters are installed in one single cabinet. The components SMGW and meter may also be realized by a single physical device providing functionality of both.

From a security perspective this solution has the advantage that the communication between the gateway unit and the meters inside happens in the protected area of the box (assuming that the connection is realized wired or by optical means that are protected by the box). Anyway the communication between gateway and meters inside the box has to be encrypted.

In this context it is relevant that there is one physical unit (in form of a sealed box/cabinet) that provides an adequate level of physical protection over the Gateway, its meters and the communication channel between. However, also in this case this PP requires the implementation of an external interface for additional meters outside the box that is protected by cryptographic functionality.

Fig. 5 acknowledges that there may be functional aspects in the context of a SMGW that are essential for the overall operation of the SMGW but not required to en-

force the security functionality of the SMGW. Those functionalities may also be implemented in form of external components that do not belong to the SMGW. Classic examples of such functionality are the communication capabilities to the WAN, LMN or HAN. As long as the requirements for separate networks, encryption and so forth are implemented within the Gateway TSF it may be possible to utilize an external communication component. A failure of such a component would of course lead to an inoperative Gateway. However–as the availability of the Gateway is not within the focus of the requirements in this PP – this would not violate any security requirement.

The requirements around physically separated interfaces for different networks also apply to this configuration as indicated by the multiple arrows between the SMGW and its external communication components.

C. HW Selection–Security Module

There already is a good number of TPM products available. This also includes microprocessor units, such as i.mx6 from Freescale being suitable candidates for high-end SMGW platforms [http://cache.freescale.com/ .. files/32bit/doc/fact_sheet/IMX6SRSFS.pdf]. They may come with ARM TrustZone support, enabling functionality like secure boot, secure storage, random number generator, and many more.

However, it seems reasonable to select a device, which already comes with the CC-certification EAL4+ to save this additional effort. For the time being this might be a TPM from Infineon (SLB9635 TT 1.2, [http://www.infineon.com/dgdl/TPM_Certification_Product-Brief.pdf?folderId=db3a3043243b5f170124a48425b0409e&fileId=db3a304329a0f6ee0129ac228ec35668] or AT-VaultIC460 from Inside Secure [http://www.insidesecure.com/eng/content/download/ … . .904/8564/version/2/file/6606AS_VIC_VaultIC460.pdf].

D. SW Architecture

The same requirement holds true with regard to the software platform. Looking at the requirements for the certification, which include white box analysis, there might be three general alternatives:

- Use a dedicated communication stack, like emBetterSSL from the authors' team [http://www.stzedn.de/embetter-webserver.132.html], which is completely available in source code and under full control.
- Second alternative would be the use of a standard Linux, which already comes with a reasonable security level, but which would cause a major significant effort to go through the certification process.
- Third alternative would be the direct use of EAL4+ certified OS, like QNX.

E. Discussions

The discussions about the hardware and the software platform lead to the simple and not at all new insight that it is very reasonable to use pre-developed and pre-certified products. Thus, cost per piece might go up, but eventually development and certification cost would be significantly reduced.

V. Cost Benefit Analysis

A. Introductory Remarks

It is obvious that the additional requirements from ch. III cause additional cost. It is clear that security is not a function as such, but it also should be clear that without the provision of security, no functionally safe operation could be achieved. In addition, data security and privacy are required for user acceptance, both from utility and consumer side.

Therefore, security is a sine qua non for the market success and for the stable and safe operation of a large scale network.

On the cost side, the Total Cost of Ownership (TCOO) during the complete lifetime is to be considered, including complete investment, installation and operational costs.

B. Cost Analysis–Devices

On the meter and the gateway sides, additional hardware resources are required for the implementation of the symmetric and possibly the asymmetric cryptography. The meter requires small amount of additional RAM and flash memory, the gateway itself requires the security module.

Consequently, there is no doubt about a certain cost adder; however, if this adder is put into relation to the total cost, including housing, logistics, and replacement (installation), it will be in the range of around 5 %.

Another critical issue comes from the energy adder for the additional data exchange and the additional computations. Especially for the generation of new key, this might be significant. With the continuing progress of semiconductor scaling, the energy spent in the microcontroller remains negligible in comparison with the energy spent for the communication part.

C. Cost Analysis–Complexity of Network and Operations

In general, higher cost should be expected due to the increasing complexity of the network and its operation. In conjunction with the increased exchange of data, e.g. with TLS, long frames or multiple fragmented frames are required, which leads to a higher load of the communication channel and of the required energy spent for the communication.

In addition, the administration processes during the commissioning and the operational phases will play a significant part. Keys shall be administrated, distributed, and kept up-to-date; role concepts shall be developed and implemented; monitoring shall be pursued.

D. Cost Analysis – Development

Additional cost will be observed also in the development and the certification process. Again, this adder has

to be understood from the global context. Many companies already follow intense internal processes, which are in big parts identical to the given requirements. And if this is not the case, yet, then it is reasonable to start their definition and implementation. Having in mind the complexity of a stable product support for many generations, companies anyhow will not go without a reasonable process.

One further aspect will be observed: The certification process will lead to longer product life cycles, shorter iterations cannot be supported. This effect could be observed in many other application fields, e.g. in medical technology or air and space technologies. Although it was anticipated that this effect would hinder innovation, it at the same time led to more stable products and more consolidated processes.

ACKNOWLEDGMENT

The authors wish to thank the colleagues from SSV Embedded Software GmbH for their support in a joint project, being supported in part by a grant from German Federal Ministry of Economy and Technology (BMWi) ZIM KF2471305ED2.

REFERENCES

[1] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks", *IEEE Communications Magazine*, vol. 50, no. 8, pp. 24-29, August 2012.
[2] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, pp. 1344–1371, 2013.
[3] R. Lu, H. Li, and R. Jiang. Bibliography on secure smart grid communications. [Online]. Available: http://bbcr.uwaterloo.ca/~rxlu/securesmartgridbib
[4] A.C. Chan and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 58-65, January 2013.
[5] CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Information Security*, November 2012.
[6] IEC Standard, IEC 62351: Data and Communication Security.
[7] National Electric Sector Cyber Security Organization Resource, *Smart Energy Profile (SEP) 1.x Summary and Analysis*, Version 1.0, October 31, 2011.
[8] Open Metering System Specification, Volume 2, Primary Communication, OMS, Issue 3.0.1, Jan 29, 2011.
[9] Open Metering System, *Technical Report 01–Security*, Issued 1.1.0, December 20, 2012.
[10] Federal Office for Information Security, *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*, Version 1.2, March 2013.
[11] Federal Office for Information Security, *Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)*, Version 1.0, March 2013.
[12] R. Oppliger, "SSL and TLS: Theory and Practice," *Artech House*, 2009.
[13] S. Jaeckel, N. Braun, and A. Sikora, "Design strategies for secure embedded networking," in: Workshop "Long-term security," in: A. U. Schmidt, M. Kreutzer, R. Accorsi (Hrsg.), "Long-term and Dynamical aspects of information security: Emerging trends in Information and communication security," Nova Science Publisher, 2007.
[14] Trusted Computing Group. [Online]. Available: https://www.trustedcomputinggroup.org

Axel Sikora holds a diploma of Electrical Engineering and a diploma of Business Administration, 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 was called into 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.

