Framework for Securing Smart Meters through Deployment of Integrated Circuits

Slobodan Bojanić, Octavio Nieto-Taladriz García and Srđan Đorđević

Abstract—**The smart meter draws today the cyber security focus as it is becoming a key node for managing information about the electricity system and final customers. In this paper, the security framework for smart meters is presented with the aim to realize their protection through cryptographically strengthened integrated circuits.**

Index Terms—**Smart meters, CMOS, side channel attacks, cyber security.**

I. Introduction

In recent decades the application and use of Information and Communication Technologies (ICT) in the Critical Infrastructures, like drinking water systems, energy grids, financial and communication infrastructures has increased enormously. These systems have opened an unforeseen amount of opportunities. Infrastructures became highly efficient and flexible, which has been beneficiary for society. In particular in the energy infrastructures, flexibility is a key to respond to the transition to intermittent sustainable power generation thus smart grids support the energy transition of the coming decades. The growing dependency on ICT also means that new threats have to be met. Threats to ICT, intentional and unintentional are a fact and growing. The disruption or destruction of electricity grids would have a serious impact on economic and societal functions. In order to keep our infrastructures resilient we have to invest in secure and resilient architectures.

Smart meter technology is a key component of the Advanced Metering Infrastructure (AMI) that will help the smart grid link the two-way flow of electricity with the two-way flow of information. Privacy and security concerns surrounding smart meter technology arise from the meters' essential functions, which include recording near-real time data on consumer electricity usage; transmitting this data to the smart grid using a variety of communications technologies; and receiving communications from the smart grid, such as real-time energy prices or remote commands that can alter a consumer's electricity usage to facilitate demand response.

Beneficial uses of AMI are developing rapidly, and like the early Internet, many applications remain unforeseen. At a basic level, smart meters will permit utilities to collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes. The meters may increase energy efficiency by giving consumers greater control over their use of electricity, as well as permitting better integration of plug-in electric vehicles and renewable energy sources. They may also aid in the development of a more reliable electricity grid that is better equipped to withstand cyber attacks and natural disasters, and help to decrease peak demand for electricity. To be useful for these purposes, and many others, data recorded by smart meters must be highly detailed, and, consequently, it may show what individual appliances a consumer is using.

Although the smart meter is becoming a key node for managing information about the electricity system and final customers, the Industrial Control Systems, and not the smart meters, still draw today the primary cyber security focus. The data must be transmitted to electric utilities subjecting it to potential interception or theft as it travels over communications networks and is stored in a variety of physical locations. Residential smart meters present privacy and cyber security issues that are likely to evolve with the technology. The issues fall into two main categories: privacy concerns that smart meters will reveal the activities of people inside of a home by measuring their electricity usage frequently over time; and fears that inadequate cyber security measures surrounding the digital transmission of smart meter data will expose it to misuse by authorized and unauthorized users of the data.

The AMI being an entrance point to the Smart Grid network for hackers/criminals; Privacy-related information in Smart Grid components / (wireless) network links of Smart Grids that is used by criminals or hackers to create reputation loss of one or more stakeholders or even TRA and/or massive technology-related distrust by citizens. Furthermore, focus on cryptography around application security and threat and vulnerability management requires significant attention because most smart grid stakeholders still have little experience in these areas. Having all this in mind, this project is planned to contribute to the security of the smart grids enforcing cryptographic capabilities of smart meters through deployment of resilient integrated circuits.

Until recently, the installed capacity of distributed generation was too low to be a critical issue in the management of the electricity distribution network.

Slobodan Bojanić is with the Escuela Técnica Superior de Ing. de Telecomunicación Universidad Politecnica de Madrid, Spain {e-mail: slobodan@die.upm.es).

Octavio Nieto-Taladriz García is with the Escuela Técnica Superior de Ing. de Telecomunicación Universidad Politecnica de Madrid, Spain {e-mail: nieto@die.upm.es).

Srdjan Djordjević is with the Electrical Engineering Department Faculty of Electronic Engineering, University of Niš, Serbia (e-mail: srdjan.djordjević@elfak.ni.ac.rs).

Zbornik 57. konferencije ETRAN, Zlatibor, 3-6. juna 2013, str. EL4.1.1-4
Proceedings of 57th ETRAN Conference, Zlatibor, Serbia, June 3-6, 2013, pp. EL4.1.1-4

II. Security Concerns

Smart grids have been defined by the European Smart Grid Task Force as electricity networks that can efficiently integrate the behaviour and actions of all users connected to it - generators, consumers and those that do both - in order to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply.

Smart grids have an essential role in the process concerning the integration of variable distributed resources in the electricity networks (key driver to get 2020 targets) and providing a user-oriented service, supporting the achievement of these targets.

Current developments on the power networks, such as digital communication between supplier and consumer, intelligent metering and monitoring systems, will allow smart grids to improve the control over electricity consumption and distribution substantially to the benefit of consumers, electricity suppliers and grid operators. Advanced Information and Communication Technologies (ICT) are at the core of an effective smart grid implementation where also industrial control systems (ICS) and related operational technology (OT) need to be taken into account. All processes across the whole value chain are heavily based on these infrastructures and technologies. Smart grids give clear advantages and benefits to the whole society, but the dependency on ICT components (e.g. computer networks, intelligent devices, etc.), ICS (e.g. supervisory control and data acquisition systems, distributed control system, etc.), OT (e.g. firmware, operating systems, etc.) and the internet makes the society more vulnerable to malicious attacks with potentially devastating results on smart grids. This can happen in particular because vulnerabilities in smart grid related communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants.

The data must also be transmitted to electric utilities—and possibly to third parties outside of the smart grid—subjecting it to potential interception or theft as it travels over communications networks and is stored in a variety of physical locations. Major security concerns regarding AMI cyber security are loss of controllability over AMI devices, followed by loss of observability due to a lack of data integrity. Cyber threats specific to AMIs included meter compromise and massive remote disconnects. Indeed, meters, along with pole-top collectors, are the components that are most vulnerable to cyber intrusion by an external entity, while the head- end system and vendor access are seen as the most vulnerable to insider attacks. Furthermore, there are concerns with respect to the following security events: unauthorized massive remote disconnect, device tampering: malware and malicious code injection (e.g., through buffer overflow attack attacks), rogue device attachment, meter tampering, access to

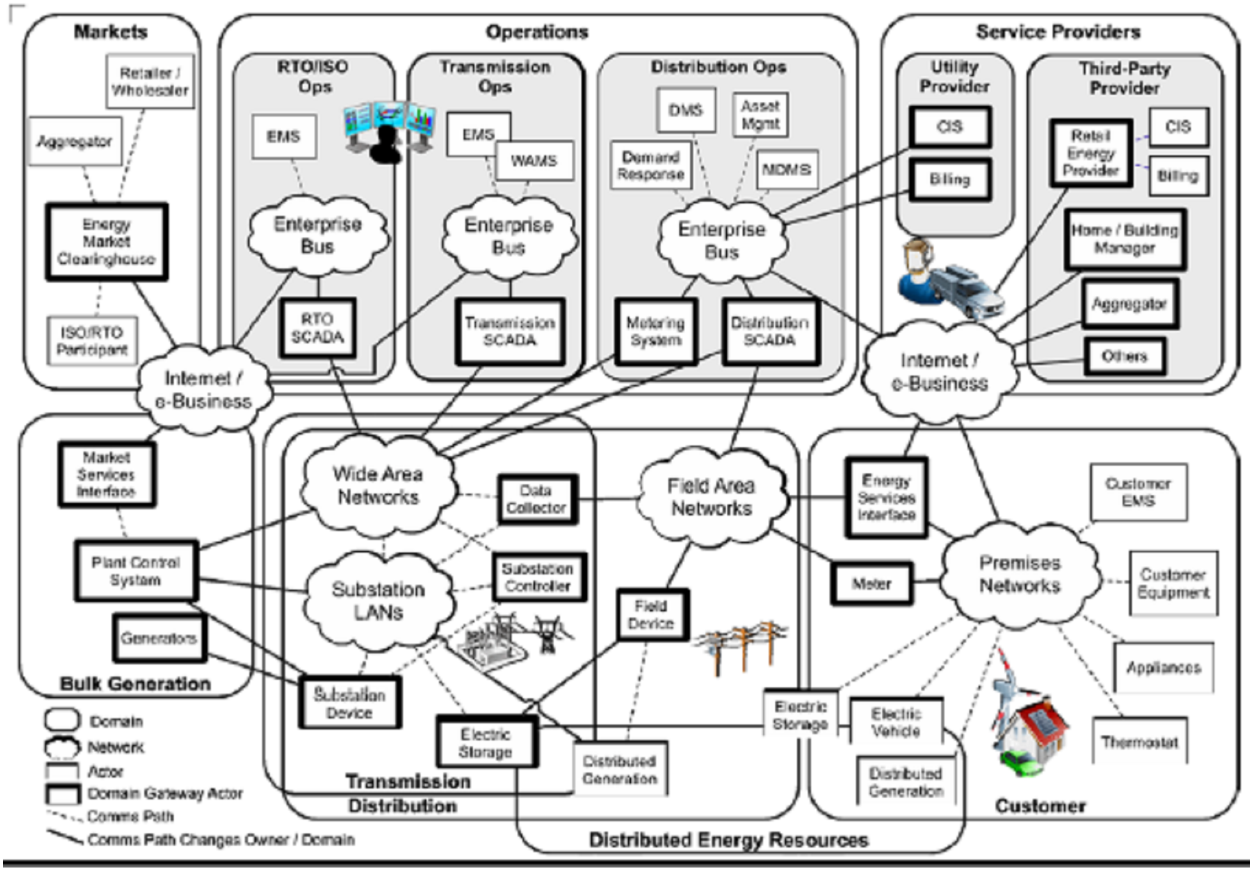

Fig. 1. Conceptual Reference Diagram for Smart Grid Information Networks [1]

firmware password, and zero-day attacks against AMI devices, cryptographic issues: access to decryption keys or discovery of flaws in encryption, denial of service against routers or cell relays, and unauthorized modifications to system configurations and physical components.

Some highly-visible examples of attacks to Smart Grids from the threats identified above: Deliberate energy market manipulation by changing Smart Grid information about the power demand or supply in a stressed market; A physical and/or cyber attack on a (small set of) single-point-of-failure Smart Grid component(s); Technology Related Anger (TRA) of Smart Grids amplified by a very active (set of) individual(s), e.g. peoples sending tweets like 'Smart Grid equipment radiation is deadly', while lacking a convincing mitigation strategy; Organized crime manipulating larger sets of consumer premises Smart Grid components or at the data concentrators, e.g. turning a large set of smart appliances off; Fraudulent information about demand or supply causing automatic measures taken which try to deal with non-existing power flows so result may be a blackout and/or high financial losses;

The smart meter is becoming a key node for managing information about the electricity system and final customers. However, Industrial Control Systems, and not the smart meters, draw today the primary cyber security focus.

In the European Commission's "Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment" on March 1st of 2011, a standardisation mandate is defined to support European Smart Grid deployment. It is a starting point for the normalisation of energy interoperability and will enable or facilitate the implementation in Europe of the different high level smart grid services and functionalities. Regarding security issues, the mandate states "A secure and robust energy network is essential for the continuous improvement and industrious operation of the European energy markets. This will only be possible if the associated information and communication networks are secure and robust." Moreover, the "Commission Recommendation of 9 March 2012, on preparations for the roll-out of smart metering systems , (2012/148/EU)" in its article 27 notes that "Member States should ensure that network operators identify security risks and the appropriate security measures for smart grids to guarantee the adequate level of security and resilience of the smart metering systems."

The applications of advanced digital technologies (i.e., microprocessor-based measurement and control, communications, computing, and information systems) are expected to greatly improve the reliability, security, interoperability, and efficiency of the electric grid, while reducing environmental impacts and promoting economic growth. Achieving enhanced connectivity and interoperability will require innovation, ingenuity, and different applications, systems, and devices to operate seamlessly with one another, involving the combined use of open system architecture, as an integration platform, and commonly-shared technical standards and protocols for communications and information systems. To realize Smart Grid capabilities, deployments must integrate a vast number of smart devices and systems**.**

Security – Architectures should support the capability to resist unwanted intrusion, both physical and cyber. This support must satisfy all security requirements of the system components. (This is covered in more detail in Chapter 6.).

The interface between the Smart Grid and the Customer domain is of special importance as the most visible part of this domain. The conceptual reference model (see Figure 3-2) depicts two distinct elements that together provide the interface to the Customer Domain: The Meter, and The Energy Services Interface (ESI), which serves as the gateway to the Customer Premises Network.

Through these interfaces, electricity usage is measured, recorded, and communicated; service provisioning and maintenance functions are performed (such as remote connection and disconnection of service); and pricing and demand response signaling occurs.

New and innovative energy-related services, which we may not even imagine today, will be developed and may require additional data streams between the Smart Grid and the Customer domain. Extensibility and flexibility are important considerations. The interface must be interoperable with a wide variety of energy-using devices and controllers, such as thermostats, water heaters, appliances, consumer electronics, and energy management systems. The diversity of communications technologies and standards used by devices in the Customer domain presents a significant interoperability challenge. In addition, ensuring cybersecurity is a critical consideration.

III. IC Design Framework

In order to realize the protection of smart meter through the hardware approach, it is necessary to carry out the specification phase where the requirements for a library of side-channel-attack (SCA) hardened digital CMOS logic cells [2]. Furthermore it is necessary to define lightweight, low-power cryptographic algorithms and communication protocols for AMI environment to be deployed [8]-[9].

In the Development phase it is expected that the synthesis of the encryption chip specified in the previous phase and then design and sample creation in the CMOS technology that is viable through the use the EUROPRACTICE services. The Verification phase consists in the design and implementation of a test system for verification of its electrical and electronic functionality. It should be followed by the the measurement and characterization of the side-channel emanations (magnetic and electrical) of the designed chip. In the last phase it is necessary to carry out the testing of cryptographic and data processing functionality.

To resume, the there are two preparatory activities. One is to develop a digital CMOS infrastructure for design of SCA resistive ICs. The second is to select the data encryption algorithms and communication protocols that would enable data protection in the communication between the metering device and the utility. Next, the results of these two activities converge into a design (based on CADENCE IC design platform) of the layout of an IC, samples of which are to be produced thanks to the EUROPRACTICE services. Finally, all ideas implemented during the preparatory and design phases are to be verified in two steps. The first one is to verify the electrical and electronic functionality of the design. In this step one may find that, for example, faulty design was produced due to a designer error. In the second and final step, the immunity of the design to SCA will be evaluated and level of effectiveness of the implemented ideas will be established. Proper highly specialized equipment and software is to be implemented for a success of this activity.

Furthermore, it should be emphasized that there is no library of digital CMOS cells hardened to side channel attack that is available to purchase. Neither many research laboratories have the proper expertise to integrate the metering chip and the new criptographic chip on a single pelet that would reduce price and rise the performances.

Therefore it is possible to enhance the security of energy infrastructure through the development of a library of digital CMOS cells which are strengthened against Side Channel Attacks and which serve as a basis for future versions of cryptographic chips that will meet new requirements and new challenges and to contribute to the cyber security practice through deployment of secure communication and establishing secure protocols and data encryption which are challenges from whose solutions will benefit the whole community.

IV. Conclusion

The deployment of Advanced Metering Infrastructure (AMI) technology significantly increases the attack surface that utilities have to protect. As a result, there is a critical need for efficient solutions to supplement protective measures and keep the infrastructure secure.

The deployment of Advanced Metering Infrastructure (AMI) technology significantly increases the attack surface that utilities have to protect. As a result, there is a critical need for efficient solutions to supplement protective measures and keep the infrastructure secure. Although the smart meter is becoming a key node for managing information about the electricity system and final customers, the Industrial Control Systems, and not the smart meters, still draw today the primary cyber security focus.

Namely, the Smart grid architecture involves many cyber assets, where some have been part of the grid for a while and others are new “smarter” assets. The project addresses the “smart” assets i.e. Advanced Metering Infrastructure thus distinguishing it from the “traditional” cyber assets i.e. SCADA. These Smart Cyber assets are new Smart Asset category which includes new monitoring and control devices, communication infrastructures, etc., which add a whole new set of capabilities for the Grid Assets to utilize. The smart movement opens the grid to vulnerabilities that already exist in the ICT world, and now those vulnerabilities pose threat to the Smart Grid (and SCADA) communications and applications also. This is a new category, which has influence mostly on all core component layers. They contribute in automation of processes and increased controllability of the grid. Consequently they increase the risk in the overall grid considerably due to the large numbers of the devices, and their collective impact. Their impact can be in any or multiple layers hence the security mechanisms need address other vectors as well.

The immunity against side channel attacks will be additionally and substantially raised due to the design of a chip that performs simultaneously the metering and cryptographic operations thus the supply current and electromagnetic emanations of such a device contain the components of analog, computational and cryptographic origin that makes difficult to recognize the ones related solely to the encryption algorithm. That needs to perform EMC/I measurements for a frequency range of several GHz and make this infrastructure available to master and doctoral students in the near future.

Acknowledgment

The work is partially supported through the bilateral scientific project financed by the Spanish and Serbian Ministries of science (“Data security in distributed measurement systems“, Spanish Ministry of Science Ref. No. PRI-AIBSE-2011-1168)

References

[1] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, February 2012

[2] M. Stanojlovi¢ and P. Petkovic, Design and simulation of multiplexer cell resistant to side channel attacks. INDEL 2012.

[3] Slobodan Bojanić, Srdan Đorđević and Octavio Nieto-Taladriz, „*Privacy Issues in Smart Grids*”, SSSS 2012**.**

[4] European Network and Information Security Agency (ENISA), “Smart Grid Security Recommendations for Europe and Member States”, 01-07-2012.

[5] Commission of the European communities. “Smart Grids: from innovation to deployment”. COM(2011) 202 final. 2011.

[6] National Institute of Standards and Technology (NIST). NISTIR 7628: Guidelines for Smart Grid Cyber Security. Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG). 2010.

[7] A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the SMART METER , October 2011.

[8] Adi Shamir, “Identity-Based Cryptosystems and Signature Schemes” Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53, 1984

[9] D. Boneh and M. K. Franklin “Identity-based encryption from the weil pairing,” CRYPTO’01 Proceedings of the 21 st Annual International Cryptology Conference and Advances in Cryptology, London, 2001, pp. 213-229.

[10] S.H.M. Kwok, E.Y. Lam, and King-Shan Lui “Zero-configuration Identity-based Signcryption Scheme for Smart Grid,” Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference, 4-6 Oct. 2010, pp. 321-326..