

# Security Engineering Methodology for Embedded Systems in Metering

Von der Naturwissenschaftlich-Technischen Fakultät  
der Universität Siegen

zur Erlangung des akademischen Grades

**Doktor der Ingenieurwissenschaften  
(Dr.-Ing.)**

genehmigte Dissertation

von

**Dipl.-Inform. Donatus Weber**

1. Gutachter: Univ.-Prof. Dr. rer. nat. Christoph Ruland
  2. Gutachter: Prof. Dr.-Ing. habil. Roman Obermaisser
- Vorsitzender: Univ.-Prof. Dr.-Ing. Horst Bessai

Tag der mündlichen Prüfung: 29.11.2013



**UNIVERSITÄT SIEGEN** 

**Institut für  
Digitale Kommunikationssysteme**

**Forschungsberichte**

Herausgeber: Univ.-Prof. Dr. Christoph Ruland

Band 29

**Donatus Weber**

---

**Security Engineering  
Methodology for Embedded  
Systems in Metering**

---

**SHAKER  
VERLAG**

Aachen 2014

**Bibliographic information published by the Deutsche Nationalbibliothek**

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

Zugl.: Siegen, Univ., Diss., 2013

Copyright Shaker Verlag 2014

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publishers.

Printed in Germany.

ISBN 978-3-8440-3078-5

ISSN 1614-0508

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen

Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9

Internet: [www.shaker.de](http://www.shaker.de) • e-mail: [info@shaker.de](mailto:info@shaker.de)

FOR CHRISTINA AND LYSANDER



# Abstract

Ongoing changes in the energy sector are leading to a need for decentralized energy supplies to enable use of green energy and reduce carbon dioxide emission. An efficient usage of these resources requires up-to-date information on the energy currently generated and consumed. The necessary infrastructure is provided by the smart grid, an intelligent network to control energy producers and consumers as well as storage.

Important components of the smart grid are intelligent metering systems with the capability of sensing measurements and communicating these to remote entities. Meters with these extended features, so called smart meters, are usually operated by embedded systems. Their communication units, referred to as gateways, provide connectivity to different networks. In operation, smart meters generate security and safety relevant as well as privacy sensitive data and transmit them over possibly insecure networks. A special protection of this data is therefore strongly required.

This circumstance was recognized by the German government in 2010 and induced the development of a Common Criteria Protection Profile for the gateway of a smart metering system by the German Federal Office for Information Security. This gateway Protection Profile is a first approach to establish security by design in the metering domain.

Newly developed gateway devices need to undergo a Common Criteria evaluation and certification before being deployed on the market. The metering domain, traditionally conservative, is now directly faced with software development processes and appropriate development documentation mandatory for a successful evaluation. Security engineering has become a key point in the metering system development. Beyond this, the complexity of metering systems is steadily increasing requiring modern development methods that allow reuse of security solutions to support cost efficiency and reduce development time.

---

The solution presented in this thesis encountering the mentioned problems is a security engineering methodology that combines key element concepts to provide security expert knowledge in different phases of the metering system development process.

Software patterns are a well-known technique to capture expert knowledge as solutions to commonly occurring problems. The security by design principle requires security to be taken into account even from the beginning of the development process. Combining security software patterns with Model Driven Engineering (MDE) techniques introduces the possibility to apply these patterns even in high level design phases of the system. Patterns are therefore stored in a model based repository offering a model transformation back-end to various domain specific development tool sets, which in turn are dedicated for use in different phases of the development process. With this precondition already established engineering processes and process tooling of companies do not need to undergo major changes with the result of widening the industry acceptance of the methodology. Furthermore security patterns may undergo a formal validation to verify the security properties provided by this solution.

Within this work a security engineering methodology applicable to embedded device development in the metering domain is developed by uniting the mentioned key concept elements. This comprises the definition of a development process with Common Criteria elements as well as the derivation and definition of security patterns dedicated for smart meter gateways.

The methodology is evaluated by applying the elements to a proof of concept gateway demonstrator. Furthermore a detailed insight into legal framework conditions as well as state of the art in market and regulatory environment of the metering domain is given.

# Zusammenfassung

Der derzeitige Wandel im Bereich der Energiewirtschaft bedingt eine Umstrukturierung in Richtung dezentrale Energieversorgung, um erneuerbare Energien effizient nutzen zu können und den Kohlenstoffdioxidausstoß zu reduzieren. Für die erfolgreiche Einbindung dieser regenerativen Energieträger sind genaue Informationen über Verbrauch und Erzeugung unabdingbar. Die dafür notwendige Kommunikationsinfrastruktur wird vom Smart Grid, einem intelligenten Energieverteilnetz zur Verfügung gestellt. Dieses Netz bietet die notwendige Funktionalität, um Energieerzeugung, -verbrauch und -speicherung aufeinander abzustimmen.

Wichtige Komponenten dieses Smart Grid sind intelligente Zählersysteme, die in der Lage sind, gewonnene Messwerte mit Fernauslesestellen zu kommunizieren. Moderne Zählersysteme mit diesen Eigenschaften, im Volksmund als Smart Meter bezeichnet, sind immer leistungsfähigere eingebettete Systeme. Sie verfügen über Kommunikationseinheiten (Gateways) mit Anbindung an verschiedene Weitverkehrsnetze. Im stationären Betrieb kommunizieren diese Zähler Datensätze, die sowohl sicherheitskritisch einzustufen sind als auch datenschutzrechtlich als brisant gelten. Solch sensible Daten müssen in besondere Weise geschützt werden. Die deutsche Bundesregierung hat diese Umstände 2010 erkannt und daraufhin die Entwicklung eines Common Criteria Protection Profiles für Gateways von Zählersystemen durch das Bundesamt für Sicherheit in der Informationstechnik in Auftrag gegeben. Dies ist der erste Schritt für die Einführung des Security by Design Prinzips im Bereich des Messwesens.

Neu entwickelte Smart Meter Gateways müssen eine Evaluation nach Common Criteria durchlaufen, bevor sie zertifiziert auf den Markt gebracht werden dürfen. Das Messwesen, als traditionell konservativer Sektor mit Ausrichtung in den elektrotechnischen Bereich, ist nun direkt mit Entwicklungsprozessen für Software und der notwendigen Entwicklungsdokumentation im Rahmen der Common Cri-

---

teria Evaluation konfrontiert, die für eine erfolgreiche Zertifizierung unumgänglich ist. Security Engineering ist zuletzt damit zu einem wichtigen Bestandteil im Entwicklungsprozess für moderne Zählersysteme geworden. Darüber hinaus werden Systeme zunehmend komplexer, was wiederum moderne Entwicklungsmethoden erforderlich macht, welche die einfache Integration und die Wiederverwendbarkeit von Sicherheitslösungen erlaubt, um kosteneffizient zu arbeiten und Entwicklungsaufwand und -zeit gering zu halten.

Die in dieser Arbeit aufgezeigte Lösung zur beschriebenen Problematik basiert auf einer Security Engineering Methodik, die verschiedene Schlüsselemente miteinander kombiniert, um in den verschiedenen Phasen des Entwicklungsprozesses eines Zählersystems IT-Security Fachwissen zur Verfügung zu stellen.

Software Pattern sind eine wohlbekannte Technik, um Expertenwissen in Form von generischen Lösungen für häufig auftretende Problemstellungen zu erfassen und Entwicklern zur Verfügung zu stellen. Dies lässt sich direkt auf Security Pattern übertragen. Das Security by Design Prinzip bedingt die Integration von Security Engineering Elementen in den gesamten Entwicklungsprozess eines Produktes und dies von Beginn an. Kombiniert man Software Pattern mit Model Driven Engineering Techniken bietet dieser Ansatz die Möglichkeit, Pattern schon in frühen Designphasen anzuwenden, um die höheren Ebenen hierfür zu erschließen.

Hierfür sind die Security Pattern in einem modellbasierten Repository hinterlegt. Eine dazugehörige Anwendung bildet die Schnittstelle zwischen Repository und den in den verschiedenen Phasen des Entwicklungsprozesses eingesetzten Werkzeugen. Diese verfügt über ein Transformationsbackend, um die modellbasierte Artefakte direkt in die verschiedenen Entwicklungswerkzeuge einzubringen. Dies bietet die Möglichkeit, die Methodik auf bereits etablierte Entwicklungsprozesse und Abläufe in Firmen anzuwenden, ohne diese grundlegend ändern zu müssen. Die in dieser Arbeit definierte Methodik vereint die genannten Schlüsselemente und optimiert diese für die Anwendung im Bereich der eingebetteten Systeme im Messwesen. Dies umfasst neben der Definition eines detaillierten Entwicklungsprozesses mit Common Criteria Elementen auch die Implementation von typischen Security Pattern für einen Smart Meter Gateway. Ein Machbarkeitsnachweis evaluiert die Methodik abschließend am Beispiel eines Smart Meter Gateway Demonstrators.

# Acknowledgment

This doctoral thesis contains results of research undertaken at the Chair for Data Communications Systems at the University of Siegen. Work on this thesis has been carried out during my employment as research assistant and has been supported by the research project Trusted Computing Engineering for Resource Constrained Embedded Systems Applications (TERESA) of the European Union.

I am most grateful to my supervisors, Univ.-Prof. Dr. rer. nat. Christoph Ruland and Prof. Dr.-Ing. habil. Roman Obermaisser. Special thanks to the chairman of my committee Univ.-Prof. Dr.-Ing. Horst Bessai and Prof. Dr.-Ing. Günter Schröder, who agreed to be my third thesis reviewer.

Furthermore I am thankful to my former colleagues Markus Dunte, Stephan Meyer, Hendrik Brandenburger, André Groll, Jan Holle, Christian Bodenstedt, Rainer Schick, Matthias Schneider, Andreas Schantin, Jinsuh Shin and Obaid Ur-Rehman for our many informal discussions.

Finally I would like to thank my family. The encouragement and support from my beloved wife Christina and our always positive and joyful son Lysander is a powerful source of inspiration and energy. These years have been a challenging trip, with both ups and downs. Fortunately, I was not alone on this road.

A special thought is devoted to my parents Jovita and Günter for a never-ending support throughout my life.



# Contents

|                                                                         |            |
|-------------------------------------------------------------------------|------------|
| <b>Abstract</b>                                                         | <b>I</b>   |
| <b>Zusammenfassung</b>                                                  | <b>III</b> |
| <b>Acknowledgment</b>                                                   | <b>V</b>   |
| <b>1 Introduction</b>                                                   | <b>1</b>   |
| 1.1 Modern Metering Systems . . . . .                                   | 1          |
| 1.2 Metering Domain Evolution . . . . .                                 | 3          |
| 1.3 Motivation . . . . .                                                | 5          |
| 1.4 Objective . . . . .                                                 | 8          |
| 1.5 Solution . . . . .                                                  | 9          |
| 1.5.1 Identification of Key Elements . . . . .                          | 9          |
| 1.5.2 Holistic Model . . . . .                                          | 13         |
| 1.6 Document Structure . . . . .                                        | 15         |
| <b>2 Metering Domain Background and Characteristics</b>                 | <b>17</b>  |
| 2.1 Electricity Metering Evolution . . . . .                            | 17         |
| 2.2 Laws, Standards and Directives . . . . .                            | 20         |
| 2.2.1 Situation in Europe . . . . .                                     | 20         |
| 2.2.2 Situation in Germany . . . . .                                    | 24         |
| 2.2.3 The Protection Profile for a Smart Meter Gateway . . . . .        | 27         |
| 2.3 Smart Grid . . . . .                                                | 35         |
| 2.4 Stakeholders and Roles . . . . .                                    | 40         |
| 2.5 State of the Art of Smart Metering System Development . . . . .     | 42         |
| <b>3 Fundamental Principles of the Security Engineering Methodology</b> | <b>45</b>  |
| 3.1 Embedded Systems . . . . .                                          | 45         |

|          |                                                          |           |
|----------|----------------------------------------------------------|-----------|
| 3.2      | Model Driven Engineering . . . . .                       | 48        |
| 3.3      | Software Patterns . . . . .                              | 54        |
| 3.4      | Process Models . . . . .                                 | 60        |
| 3.5      | Formal Methods . . . . .                                 | 64        |
| 3.5.1    | Formal Validation Techniques . . . . .                   | 64        |
| 3.5.2    | The Security Modeling Framework (SeMF) . . . . .         | 65        |
| <b>4</b> | <b>Related Work</b>                                      | <b>67</b> |
| 4.1      | Security Engineering . . . . .                           | 67        |
| 4.1.1    | Information Security Engineering . . . . .               | 67        |
| 4.1.2    | Common Criteria . . . . .                                | 71        |
| 4.2      | Smart Metering and Smart Grid Security . . . . .         | 78        |
| 4.2.1    | Attacks and Motivation . . . . .                         | 78        |
| 4.2.2    | Privacy Concerns . . . . .                               | 80        |
| 4.2.3    | Security for Smart Metering Systems . . . . .            | 82        |
| 4.3      | Research Project TERESA . . . . .                        | 83        |
| <b>5</b> | <b>Security Engineering Methodology</b>                  | <b>85</b> |
| 5.1      | Methodology Components . . . . .                         | 85        |
| 5.2      | Security Patterns . . . . .                              | 85        |
| 5.2.1    | Pattern Structure and Contents . . . . .                 | 85        |
| 5.2.2    | Pattern Instantiation and Integration . . . . .          | 89        |
| 5.2.3    | Formal Validation of Patterns . . . . .                  | 90        |
| 5.2.4    | Pattern Creation Process . . . . .                       | 91        |
| 5.2.5    | Pattern Linkage . . . . .                                | 93        |
| 5.3      | Security Pattern Repository . . . . .                    | 96        |
| 5.4      | Repository Tools . . . . .                               | 98        |
| 5.4.1    | Pattern Search and Instantiation Tool . . . . .          | 98        |
| 5.4.2    | Keyword Search . . . . .                                 | 99        |
| 5.4.3    | Context Based Search . . . . .                           | 100       |
| 5.4.4    | Pattern Browser . . . . .                                | 101       |
| 5.4.5    | Pattern Export History . . . . .                         | 102       |
| 5.4.6    | Pattern Upload and Repository Maintenance Tool . . . . . | 103       |

|          |                                                                                            |            |
|----------|--------------------------------------------------------------------------------------------|------------|
| 5.5      | Engineering Process . . . . .                                                              | 104        |
| 5.5.1    | Methodology Integration . . . . .                                                          | 104        |
| 5.5.2    | Metering Domain MDE Tooling . . . . .                                                      | 105        |
| <b>6</b> | <b>Security Patterns and Engineering Process</b>                                           | <b>107</b> |
| 6.1      | Selection of Smart Meter Gateway Patterns . . . . .                                        | 107        |
| 6.2      | Smart Meter Gateway Security Patterns . . . . .                                            | 109        |
| 6.2.1    | Secure Remote Readout . . . . .                                                            | 109        |
| 6.2.2    | Wake up Service . . . . .                                                                  | 115        |
| 6.2.3    | Key Manager . . . . .                                                                      | 120        |
| 6.2.4    | Secure Communication (TLS) . . . . .                                                       | 123        |
| 6.3      | Engineering Process . . . . .                                                              | 128        |
| 6.3.1    | Process Requirements . . . . .                                                             | 128        |
| 6.3.2    | Process Definition . . . . .                                                               | 129        |
| 6.3.3    | Process Model . . . . .                                                                    | 130        |
| 6.3.4    | Process Phase Descriptions . . . . .                                                       | 133        |
| 6.3.4.1  | Requirements Analysis . . . . .                                                            | 133        |
| 6.3.4.2  | System Design . . . . .                                                                    | 135        |
| 6.3.4.3  | Architecture Design . . . . .                                                              | 137        |
| 6.3.4.4  | Detailed Design . . . . .                                                                  | 139        |
| 6.3.4.5  | Implementation . . . . .                                                                   | 141        |
| 6.3.4.6  | Unit Test . . . . .                                                                        | 145        |
| 6.3.4.7  | Integration Test . . . . .                                                                 | 147        |
| 6.3.4.8  | System Test . . . . .                                                                      | 149        |
| 6.3.4.9  | Certification . . . . .                                                                    | 151        |
| 6.4      | Application Scenarios in the Metering Domain . . . . .                                     | 153        |
| 6.4.1    | Meter Manufacturing Company (International) . . . . .                                      | 153        |
| 6.4.2    | SME Meter Manufacturer . . . . .                                                           | 154        |
| 6.4.3    | Company offering Common Criteria Evaluation Services<br>for Smart Meter Gateways . . . . . | 155        |
| <b>7</b> | <b>Proof of Concept Implementation</b>                                                     | <b>157</b> |
| 7.1      | Scope of the Implementation . . . . .                                                      | 157        |

|          |                                                   |            |
|----------|---------------------------------------------------|------------|
| 7.2      | Application Characteristics . . . . .             | 157        |
| 7.2.1    | Smart Meter Gateway . . . . .                     | 157        |
| 7.2.2    | Remote Readout Center . . . . .                   | 159        |
| 7.2.3    | Functions and Use Cases . . . . .                 | 160        |
| 7.2.4    | Actors and Roles . . . . .                        | 162        |
| 7.3      | System Entities and Components . . . . .          | 164        |
| 7.3.1    | Overall System . . . . .                          | 164        |
| 7.3.2    | Hardware Platform . . . . .                       | 165        |
| 7.3.3    | Hardware Security Module . . . . .                | 167        |
| 7.3.4    | Electricity Meter . . . . .                       | 169        |
| 7.3.5    | Other Periphery . . . . .                         | 170        |
| 7.3.6    | Interfaces . . . . .                              | 170        |
| 7.4      | Gateway Demonstrator Engineering . . . . .        | 172        |
| 7.4.1    | Objective . . . . .                               | 172        |
| 7.4.2    | Requirements Analysis . . . . .                   | 172        |
| 7.4.3    | System Design . . . . .                           | 174        |
| 7.4.4    | Architecture Design . . . . .                     | 174        |
| 7.4.5    | Detailed Design . . . . .                         | 177        |
| 7.4.6    | Implementation . . . . .                          | 181        |
| 7.4.7    | Test . . . . .                                    | 182        |
| 7.5      | Gateway Functionality Check . . . . .             | 184        |
| 7.5.1    | Smart Meter Gateway Demonstrator . . . . .        | 184        |
| 7.5.2    | Displaying of instantaneous Consumption . . . . . | 186        |
| 7.5.3    | Displaying of consumed Energy . . . . .           | 187        |
| 7.5.4    | Push Service . . . . .                            | 187        |
| 7.5.5    | Wake up Service . . . . .                         | 189        |
| <b>8</b> | <b>Conclusion</b>                                 | <b>191</b> |
| 8.1      | Security Engineering Methodology . . . . .        | 191        |
| 8.2      | Comprehensive solution TLS/SSL . . . . .          | 192        |
| <b>9</b> | <b>Outlook</b>                                    | <b>195</b> |
|          | <b>List of Figures</b>                            | <b>197</b> |

|                       |            |
|-----------------------|------------|
| <b>List of Tables</b> | <b>201</b> |
| <b>Glossary</b>       | <b>203</b> |
| <b>Bibliography</b>   | <b>207</b> |