

Analysis and Evaluation of the IEC 61850 Communication Standard for Monitoring and Control of Distributed Energy Resources

Stefan Feuerhahn

Analysis and Evaluation of the IEC 61850 Communication Standard for Monitoring and Control of Distributed Energy Resources

Der Fakultät für Elektrotechnik und Informationstechnik der
Technischen Universität Dortmund
zur Erlangung des akademischen Grades eines
Dr.-Ing.

genehmigte Dissertation

von
Dipl.-Ing. Stefan Feuerhahn

Datum der Einreichung: 2017/03/20

Datum der Promotionsprüfung: 2017/06/26

Referent: Prof. Dr.-Ing. Christian Wietfeld

Korreferent: Prof. Dr. Sebastian Lehnhoff

Dortmunder Beiträge zu Kommunikationsnetzen und -systemen

Band 16

Stefan Feuerhahn

**Analysis and Evaluation of the IEC 61850
Communication Standard for Monitoring and Control
of Distributed Energy Resources**

D 290 (Diss. Technische Universität Dortmund)

Shaker Verlag
Aachen 2017

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.: Dortmund, Technische Univ., Diss., 2017

Copyright Shaker Verlag 2017

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 978-3-8440-5594-8

ISSN 1867-4879

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

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

Internet: www.shaker.de • e-mail: info@shaker.de

Abstract

A future energy regime based on more distributed and fluctuating generation requires sophisticated communication solutions to monitor and control an increasing number of distributed energy resources (DERs). Many of the necessary communication solutions require IP-based communication protocols. This work examines one important candidate for such a protocol, the IEC 61850 communication standard.

The IEC 61850 standard is a feature-rich protocol that was first solely designed for substation automation. Later its information models have been extended for different DER types. By now it is already being used to control wind power plants and CHP units among others.

This work is the first to assess in detail how well IEC 61850 is suited for the control of DERs by analyzing qualitative and quantitative aspects. The qualitative criteria comprise functionality, interoperability (through information models), security and usability. The quantitative metrics under investigation are message size (how efficiently messages are encoded) and processing performance. They are analyzed analytically and experimentally using profiling and benchmarking.

These criteria are largely influenced by the following three aspects of the standard: (1) its data model, (2) its communication mappings and (3) its implementation design. After an individual analysis of these aspects, this work presents an in-depth performance analysis. Finally, the protocol is compared to the metering protocols DLMS/COSEM and SML as well as the automation protocol OPC UA.

IEC 61850's hierarchical information model is generally regarded as a benefit over the flat address space of other protocols. The information model shall increase interoperability by enabling self-descriptive devices with uniform models. This work questions these assumptions. It is shown that several properties of the model hinder comprehension, interchangeability and ultimately interoperability. To resolve the issues, improvements are suggested and the definition of a device profile is demonstrated.

Different protocol mappings can be used to realize the abstract services defined by IEC 61850. This work compares the three mappings MMS, Web Services and XMPP with respect to functionality, security, and message size. As a result of the investigation, the remainder of this work focuses on the MMS mapping of IEC 61850.

As part of this work the author has implemented the IEC 61850 standard and published it under an open-source license as OpenIEC61850. It was the first non-commercial implementation. This work identifies different implementation design options, compares them and derives the strategy used in the author's implementation.

At the core of this work is a quantitative analysis of the performance of IEC 61850 stack implementations. The stack performance is relevant for clients running on embedded hardware in the home as well as for large-scale Internet servers controlling a large number of IEC 61850 devices.

Using profiling it was shown that ASN.1 BER encoding and decoding has a large impact on processing performance. Therefore, different ASN.1 BER coding strategies are systematically compared and major performance aspects are discussed. The best strategy was identified and implemented by the author. Using benchmarking it could be shown that the resulting implementations reach a significant performance gain.

After this analysis of particular aspects of IEC 61850, the standard as a whole is compared to the metering protocols DLMS/COSEM and SML as well as to the automation protocol OPC UA. The comparison criteria are functionality, interoperability, security, message size and processing performance.

The results of this work have been presented in several IEEE conferences as well as a journal paper. The IEC 61850 and ASN.1 BER libraries developed as part of this work are now in widespread use by companies world-wide such as Siemens, Bosch Rexroth and the European Space Agency. Among other applications the software is used for the control of wind farms and CHP-units.

Zusammenfassung

Das zukünftige Energiesystem basiert auf einer wachsenden Anzahl verteilter Erzeuger und erfordert anspruchsvolle Kommunikationslösungen für deren Steuerung. Viele der notwendigen Lösungen erfordern IP-basierte Kommunikationsprotokolle. Diese Arbeit untersucht einen wichtigen Kandidaten für ein solches Protokoll, den IEC 61850 Kommunikationsstandard.

Die Normenreihe IEC 61850 definiert ein funktionsreiches Protokoll, das zunächst ausschließlich für die Automatisierung von Umspannwerken entworfen wurde. Später wurden die Informationsmodelle für verschiedene Typen von Energieerzeugern erweitert. Mittlerweile wird der Standard unter anderem zur Steuerung von Windkraftanlagen und KWK-Anlagen eingesetzt.

Diese Arbeit bewertet die Eignung von IEC 61850 für die Steuerung von dezentralen Energieanlagen anhand qualitativer und quantitativer Kriterien. Die qualitativen Kriterien umfassen Funktionalität, Interoperabilität, Sicherheit und Benutzerfreundlichkeit. Die quantitativen Metriken, die untersucht werden, sind Nachrichtengröße und Verarbeitungszeit. Diese werden analytisch und experimentell mittels Profiling und Benchmarking analysiert.

Diese Kriterien werden weitgehend durch die folgenden drei Aspekte des Standards beeinflusst: (1) das Datenmodell, (2) die Kommunikations-Mappings und (3) die Architektur der Stack-Implementierungen. Nach einer individuellen Analyse dieser Aspekte präsentiert diese Arbeit eine umfangreiche Performance-Analyse. Schließlich wird das Protokoll mit den Zählerprotokollen DLMS/COSEM und SML sowie dem Automatisierungsprotokoll OPC UA verglichen.

Das hierarchische Informationsmodell von IEC 61850 wird allgemein als ein Vorteil gegenüber dem flachen Adressraum anderer Protokolle angesehen. Das Informationsmodell soll die Interoperabilität erhöhen, indem es selbstbeschreibende Geräte mit einheitlichen Modellen ermöglicht. Diese Arbeit hinterfragt diese Annahmen. Es wird gezeigt, dass mehrere Eigenschaften des Modells das Verständnis, die Austauschbarkeit und letztlich die Interoperabilität behindern. Zur Lösung der Probleme werden Verbesserungen vorgeschlagen und der Entwurf eines Geräteprofils wird demonstriert.

Verschiedene Protokoll-Mappings können verwendet werden, um die von IEC 61850 definierten abstrakten Dienste zu realisieren. Diese Arbeit vergleicht die drei Mappings MMS, Web Services und XMPP in Bezug auf Funktionalität, Sicherheit und Nachrichtengröße. Als Ergebnis der Untersuchung konzentriert sich der Rest dieser Arbeit auf das MMS Mapping von IEC 61850.

Im Rahmen dieser Arbeit hat der Autor den IEC 61850 Standard implementiert und unter einer Open-Source-Lizenz unter dem Namen *OpenIEC61850* veröffentlicht. Es war die erste nicht-kommerzielle Umsetzung. Diese Arbeit identifiziert und vergleicht verschiedene Softwarearchitekturoptionen. Die Ergebnisse des Vergleichs sind in die Implementierung des Autors geflossen.

Im Mittelpunkt steht eine quantitative Analyse der Performance von IEC 61850 Stack-Implementierungen. Die Stack-Performance ist relevant für Clients auf eingebetteten Systemen sowie für Internet-Server, die eine große Anzahl von IEC 61850 Geräten steuern.

Mittels Profiling zeigt die Arbeit, dass die Kodierung von ASN.1 BER-Daten einen großen Einfluss auf die Verarbeitungszeit hat. Daher werden verschiedene ASN.1 BER-Kodierungsstrategien systematisch verglichen und wichtige Leistungsaspekte diskutiert. Die beste Strategie wurde vom Autor identifiziert und implementiert. Mittels Benchmarking konnte gezeigt werden, dass die resultierende Implementierung einen signifikanten Leistungsgewinn erzielt.

Nach dieser Analyse einzelner Aspekte von IEC 61850 wird der Standard als Ganzes mit den Messprotokollen DLMS/COSEM und SML sowie dem Automatisierungsprotokoll OPC UA verglichen. Die Vergleichskriterien sind Funktionalität, Interoperabilität, Sicherheit, Nachrichtengröße und Verarbeitungszeit.

Die Ergebnisse dieser Arbeit wurden in mehreren IEEE-Konferenzen sowie einem Journal veröffentlicht. Die im Rahmen dieser Arbeit entwickelten Software-Bibliotheken zu IEC 61850 und ASN.1 BER werden bereits von Unternehmen wie Siemens, Bosch Rexroth und der Europäischen Weltraumorganisation genutzt. Unter anderem wird die Software zur Steuerung von Windparks und KWK-Anlagen eingesetzt.

Contents

1	Introduction	1
1.1	Motivation and Goal	1
1.2	Approach	3
1.2.1	Qualitative Criteria	3
1.2.2	Quantitative Criteria	5
1.2.3	Structure	5
2	Background	7
2.1	Communication Alternatives for DERs	7
2.1.1	Control Stakeholders	7
2.1.2	IP-based Solutions	8
2.2	Substation Automation	9
2.2.1	Components and Functions	10
2.2.2	Communication Technology	12
2.3	IEC 61850	13
2.3.1	Standardization Bodies	13
2.3.2	Historical Development	14
2.3.3	Fundamental Concepts	15
2.3.4	Conformance Testing	20
3	Interoperability through Information Models	23
3.1	Introduction	23
3.2	Modeling Terminology	24
3.3	Modeling Rules	26
3.3.1	Server	27
3.3.2	Logical Device	27
3.3.3	Logical Node	28
3.3.4	Data Object	30
3.3.5	Array	31
3.3.6	Constructed Data Attribute	32
3.3.7	Basic Data Attribute	33
3.4	Profile Modeling Demonstration	33
3.4.1	Use Case	35

3.4.2	Micro-CHP Units	35
3.4.3	Control Hierarchy	36
3.4.4	Existing CHP Unit Models	37
3.4.5	Profile Design	38
3.5	The Model's Impact on Interoperability	43
3.5.1	Human Comprehensibility	43
3.5.2	Interchangeability and Plug and Play	45
3.6	Conclusion	46
4	Service Mapping Comparison	49
4.1	Existing Mappings	49
4.1.1	MMS	50
4.1.2	Web Services	51
4.1.3	XMPP	51
4.2	Comparison	53
4.2.1	Functionality	53
4.2.2	Security	53
4.2.3	Message Size	54
4.3	Conclusion	56
5	Implementation Design	61
5.1	OpenIEC61850	61
5.2	Representation of the Information Model	62
5.3	ACSI Services as Client API Functions	64
5.4	Mappings as Plug-Ins	67
5.5	Server API Design	68
5.6	Conclusion	70
6	Performance Analysis	73
6.1	Introduction	73
6.1.1	Performance Requirements	73
6.1.2	Related Work	74
6.1.3	Approach	75
6.1.4	ASN.1 and BER	75
6.2	MMS PDU Size	76
6.2.1	PER Instead of BER	76
6.2.2	Overhead Caused by the OSI Stack	77
6.3	Performance Profiling	79
6.3.1	Java Performance	81
6.3.2	Measurement Setup	82
6.3.3	Results	83
6.4	BER Coding Strategies	83
6.4.1	Coding Without the ASN.1 Definition	84

6.4.2	Coding Using the ASN.1 Definition	85
6.4.3	Tree Structure vs. Stream	86
6.4.4	Choosing a Strategy for IEC 61850 MMS	88
6.5	jASN1 - an Efficient BER Coder	90
6.5.1	Motivation	90
6.5.2	Compiler	91
6.5.3	Performance Optimization	91
6.5.4	Performance Comparison	92
6.6	Stack Performance	94
6.7	Conclusion	97
7	Comparison with Metering Protocols	99
7.1	Introduction	99
7.1.1	IEC 61850 for Metering	100
7.1.2	DLMS/COSEM	100
7.1.3	SML	100
7.2	Comparison	101
7.2.1	Functionality	101
7.2.2	Interoperability Through Information Models	103
7.2.3	Message Size	105
7.3	Conclusion	108
8	Comparison with OPC UA	111
8.1	OPC UA	111
8.2	Comparison	113
8.2.1	Functionality	113
8.2.2	Interoperability Through Information Models	116
8.2.3	Security	119
8.2.4	Message Size	122
8.2.5	Processing Performance	125
8.3	Conclusion	128
9	Conclusion	131
A	List of Abbreviations	135
B	Protocol Messages	139
C	ASN.1 Example	143
D	OPC UA Message Structures as ASN.1	145
E	Acknowledgements	149

F Scientific Activity	151
F.1 Publications	151
F.2 Supervision of Student Theses	152
Bibliography	153