Forschungsbericht WS 2012/2013

Kommunikation im Smart Grid – Kommunikationsbedarf eines MUC Controllers

Prof. Dr.-Ing. Rainer Bermbach

Einleitung

Das intelligente Stromnetz, das Smart Grid, ist als Begriff in aller Munde. Spätestens seit dem beschlossenen Atomausstieg in Deutschland erscheint es nun noch dringender, die Stromversorgung in Richtung mehr „Intelligenz“ umzubauen [1]. Doch was ist das Smart Grid eigentlich? Der ZVEI zusammen mit dem BDEW [2] definieren das Smart Grid wie folgt: „*Ein Smart Grid ist ein Energienetzwerk, das das Verbrauchs- und Einspeiseverhalten aller Marktteilnehmer, die mit ihm verbunden sind, integriert. Es sichert ein ökonomisch effizientes, nachhaltiges Versorgungssystem mit niedrigen Verlusten und hoher Verfügbarkeit.*“

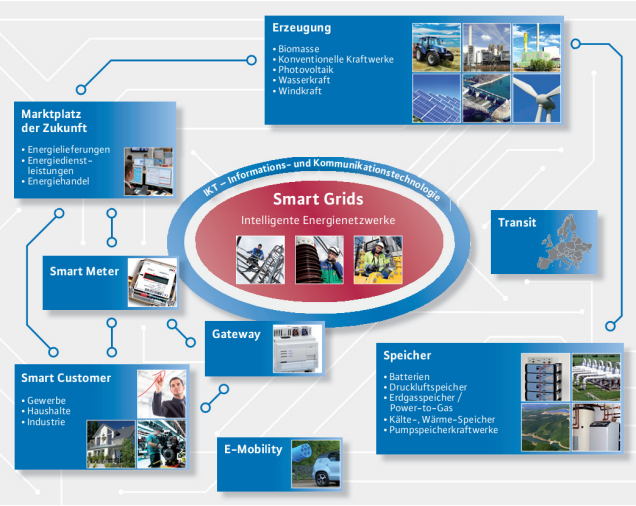

Abb. 1: Komponenten und Umfeld des Smart Grid [2]

Abbildung 1 zeigt das Umfeld, in dem sich das Smart Grid befindet. Neben den Verteilnetzen gehören dazu z.B. die vielfältigen Arten der konventionellen und regenerativen Energieerzeugung, Energiespeichertechnik, intelligente Verbrauchsmessgeräte (Smart Meter) und ihre Kopplung mit „intelligentem“ Verbrauch (Smart Consumer, Smart Home) über sog. Gateways mit dem Smart Grid. Überhaupt spielt die Informations- und Kommunikationstechnik (IKT) bei der Realisierung des Smart Grid eine zentrale Rolle. Hier wird auch von vielen Stellen ein großer Bedarf an Forschung und Entwicklung gesehen [3, 4].

Smart Metering Gateway

Das durchgeführte Forschungsprojekt konzentrierte sich im Kontext des Smart Grid auf die Anbindung der Bereiche Smart Metering und Smart Home an das Gesamtnetz. Hierzu werden Datenkonzentratoren eingesetzt, auch Multi Utility Communication (MUC) Controller genannt [5]. In zunehmendem Maße spricht man auch von Gateways, speziell auch von Smart Metering Gateways (SMGW) [6], auch wenn die Funktionalität über die Funktionalität eines klassischen Gateways (Protokollumsetzung) deutlich hinausgeht. In einigen Veröffentlichungen spricht man auch vom Communication Hub [7]. Im Folgenden wird immer der neue Begriff Smart Metering Gateway (SMGW) verwendet.

Abbildung 2 zeigt ein Smart Metering Gateway in seinem typischen Kontext. Es bildet die Schnittstelle für die Kommunikation mit dem Smart Grid. Lokal laufen alle Kommunikationsdaten bei

ihm zusammen. Primär handelt es sich dabei um die Verbindungen zum sog. Smart Metering, also zu jeder Art von Zählern, seien es moderne Stromzähler, Gaszähler oder Zähler für Wasser, Wärme etc. Hier geht es um die Messung von Verbräuchen. Aber auch die Energieerzeugungsseite ist mit Zählern bestückt, z.B. lokale Photovoltaikanlagen (PV), eventuelle Windenergieanlagen oder aber auch kleine Blockheizkraftwerke (BHKW), auch Mikro-Kraftwärmekopplung (MKWK) genannt. Diese Energiequellen werden auch mit DER (Distributed Energy Resources) bezeichnet.

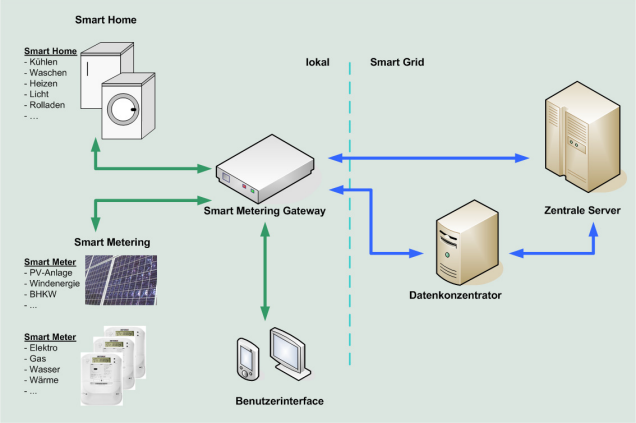

Abb. 2: Das Smart Metering Gateway in seinem Umfeld

Einen ganz anderen Bereich, der bislang, wenn vorhanden, völlig autark betrieben wurde, bildet das Smart Home. Von den vielfältigen Möglichkeiten der intelligenten Steuerung eines Haushalts sind hier insbesondere die interessant, deren Energieverbrauch in zeitlicher oder mengenmäßiger Weise gesteuert werden können. Dies sind also beispielsweise Kühlgeräte, die bei einem Übermaß an verfügbarer Energie stark herunter gekühlt werden und sich zu anderen Zeiten langsam wieder auf das Normalmaß erwärmen. Auch Waschmaschinen, Trockner und Geschirrspülmaschinen müssen nicht zu einem bestimmten Zeitpunkt laufen, sondern schlimmstenfalls zu einem fixen Zeitpunkt fertig sein. Im Rahmen der Technischen Richtlinie des BSI (s.u., [6]) werden solche Geräte unter dem Begriff CLS – Controllable Local Systems zusammengefasst.

Das Benutzerinterface für den Endverbraucher/-erzeuger sowie eine Serviceschnittstelle muss ebenfalls vom SMGW bedient werden. Hier soll der Kunde Zugriff erhalten auf seine Verbrauchsdaten etc., die u.U. auch passend statistisch aufbereitet sein können. Auch ein Servicetechniker muss über eine solche Schnittstelle Zugang zu relevanten Daten bekommen und neue Systeme konfigurieren und in Betrieb nehmen.

All diese lokalen Geräte und Anlagen fasst das SMGW kommunikationsmäßig zusammen und verbindet sie mit dem Rest des Smart Grid. Hier existieren vielfältige Verbindungen zu den verschiedensten Servern, entweder direkt oder über zwischengeschaltete Datenkonzentratoren, die die Daten vieler SMGW bündeln und dann an die entsprechenden Server weiterreichen.

Typische Protokolle in der Kommunikation des SMGW

Auf den genannten Pfaden lokal oder im Smart Grid geschieht der Datenaustausch in ganz spezifischer Weise. Während bislang im Energiebereich im Wesentlichen Punkt-zu-Punkt-Verbindungen vorherrschten und im Haushalt manuell abgelesen wurde, so ist das Smart Grid und damit ein Smart Metering nur möglich durch den Einsatz moderner Kommunikationsverfahren, die im Smart Grid und in zunehmendem Maße auch lokal TCP/IP-basiert über klassische Internettechniken abgewickelt werden.

Da „das Smart Grid“ noch nicht bzw. nur in Ansätzen und Pilotprojekten existiert, haben sich noch keine festen Protokolle einheitlich durchgesetzt. Hier geht jedes Land und jeder Betreiber offenbar seinen eigenen Weg, auch wenn es nationale und internationale Bestrebungen und Anstrengungen gibt, die eine Harmonisierung versuchen.

Die Vielfalt der Ansätze zeigt sich auch in der Art der verwendeten oder vorgeschlagenen Proto-

kolle. Sie decken die unterschiedlichsten Ebenen des OSI-Schichtenmodells ab. Somit sind sie auch nicht einfach austauschbar. Manche Protokolle decken nur die unteren Ebenen ab, andere befinden sich hauptsächlich auf der Transportschicht, wieder andere bauen eher auf anderen auf und realisieren vornehmlich die Applikationsebene. Daneben existieren vor allem im Smart-Home-Bereich Ansätze, die mehr oder weniger alle OSI-Schichten spezifizieren und abdecken. Dabei sind viele Protokolle genormt bzw. befinden sich im Standardisierungs- und/oder Erweiterungsprozess. Andere sind Quasi-Standards bedeutender Markteilnehmer oder völlig proprietär.

Eine sich herauskristallisierende Protokollfamilie ist die **IEC 61850** (DIN EN 61850). Dieses Protokoll liegt auf der Anwendungsschicht und verwendet einen modellbasierten Ansatz (ACSI – Abstract Communication Service Interface), der wiederum über weitere Protokolle wie MMS (Manufacturing Message Specification, ISO 9506) letztlich auf TCP/IP aufsetzt. Die Norm IEC 61850 stammt aus der Verteilnetzautomatisierung. Für die Kommunikation im Smart Grid ist die IEC 61850-7 relevant. Sie scheint sich in den nicht-lokalen Bereichen des Smart Grid allmählich durchzusetzen. Darüber hinaus findet sie in bestimmten Bereichen der regenerativen Energieerzeugung (DER – Distributed Energy Resources) Einsatz. Weiterhin gilt es, die in den Servern vorliegenden Informationen an die Datenbasen der übergeordneten EDV anzubinden. Dort kommt meist das Common Information Model (**CIM**, DIN EN 61970) zum Einsatz.

DLMS/COSEM (Device Language Message Specification/Companion Specification for Energy Metering) ist in der IEC 62056 spezifiziert. DLMS ist ebenfalls auf der Applikationsebene angesiedelt und beschreibt allgemeine Konzepte wie z.B. verfügbare Services. COSEM ergänzt DLMS um spezifische Objekte zur Beschreibung von Energiemessung u.ä. COSEM verwendet sog. OBIS-Kennzahlen (Object Identification System), die beispielsweise kennzeichnen, welche Energieart (z.B. Strom, Wasser, Wärme) und welcher Parameter (z.B. Wirkleistung) übermittelt werden soll. DLMS/COSEM könnte sich als das Standardprotokoll im Smart Metering lokal und zu externen Servern entwickeln. Vorteilhaft ist, dass viele Protokolle der unteren Ebenen DLMS/COSEM unterstützen und ausdrücklich vorsehen.

Eines dieser Protokolle ist der sog. **M-Bus** (EN 13757), der als Kommunikationsstandard für Zähler, Sensoren und Aktoren vorgesehen ist. Auf der physischen Ebene sind verschiedene Versionen inkludiert beispielsweise Twisted-Pair sowie der Wireless M-Bus, der im ISM-Band agiert. Er wurde im Hinblick auf einfache, kostengünstige Realisierung entwickelt, was auch Batteriebetrieb ermöglichen soll. Er könnte sich zum Standard auf den unteren Kommunikationsschichten des Smart Metering entwickeln. Im Bereich des Smart Home scheint er derzeit kaum verbreitet.

Bei den Funkstandards ist auch ZigBee bzw. **ZigBee Smart Energy** zu nennen. ZigBee arbeitet auch in den ISM-Bändern. Seine herausragende Eigenschaft ist die Selbstorganisation eines ZigBee-Netzes (Mesh). Es erlaubt auch mit DLMS/COSEM zusammenzuarbeiten und ist sowohl im Smart Metering als auch im Smart Home anzutreffen.

Ein spezielles, weitgehend nur in Deutschland verbreitetes Protokoll, um Elektrozähler anzuschließen, ist die Smart Message Language **SML** (IEC 62056-5-3-8). SML ist vergleichsweise einfach aufgebaut und kommuniziert über Zweidrahtleitungen oder auch GSM und verwendet dabei TCP/UDP. In den heute am Markt verfügbaren bzw. installierten Smart-Metering-Zählern in Deutschland ist SML weit verbreitet.

Im Smart-Home-Bereich gebräuchlich ist **KNX**. KNX möchte eine Komplettlösung für das Smart Home anbieten und ist in vielen Produkten der heute weltweit verfügbaren Home Automation

enthalten. Es stellt Modelle für verteilte Automatisierung, Konfiguration und Management zur Verfügung. KNX kann über Twisted Pair, Funk und IP kommunizieren.

Kommunikationsstandards des SMGW in der BSI TR-03109

In seiner Eigenschaft als Kommunikationszentrale eines Smart Metering Systems benötigt das SMGW erhöhte Aufmerksamkeit bezüglich der Sicherheit des Systems. Aus diesem Grund hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Auftrag des Bundeswirtschaftministeriums mit den Anforderungen an die Sicherheitsarchitektur von intelligenten Stromnetzen befasst, um sicherzustellen, dass von Anfang an Datenschutz und Datensicherheit gewährleistet werden. Eine Analyse der Bedrohungsszenarien lieferte die Grundlage für ein Schutzprofil, das alle SMGW erfüllen müssen. Um auch Interoperabilität und die geeignete technische Umsetzung des Schutzprofils zu gewährleisten, entwickelte das BSI auch entsprechende Vorgaben in einer Technischen Richtlinie (BSI TR-03109, [6]). Eine vorläufige Version (RC) publizierte das BSI am 21.12.12 und veröffentlichte nach folgenden Anhörungen kürzlich (18.03.2013) die Version 1.0 von Richtlinie und Schutzprofil (PP – Protection Profile [9]) des Sicherheitsmoduls und die Version 1.2 des Schutzprofils des SMGW [8]. Das BSI macht dort u.a. sehr umfangreiche Vorgaben für die Funktionalität und die Sicherheit eines Smart Metering Systems. (Die eichrechtlichen Belange eines solchen Systems deckt die Richtlinie PTB-A 50.7 der Physikalisch-Technischen Bundesanstalt ab [10].)

Da die Veröffentlichung der Technischen Richtlinie erst gegen Ende der Projektphase erfolgte (die endgültige Version stand sogar erst nach Projektlaufzeit zur Verfügung), konnte diese nur ansatzweise in die Betrachtung einbezogen werden.

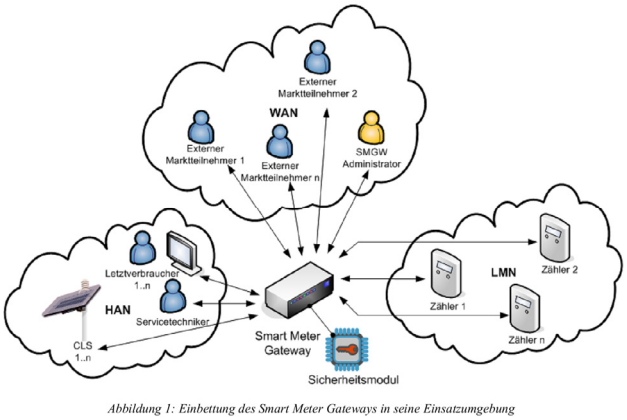

Abbildung 1: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Abb. 3: Das Smart Metering Gateway in seiner Umgebung [6]

Die TR-03109 unterscheidet kommunikations- und sicherheitstechnisch drei wesentliche Bereiche (s. Abbildung 3): Das WAN (Wide Area Network), das HAN (Home Area Network) sowie das LNM (Local Metrological Network).

Das LMN umfasst sämtliche Zähler für Verbräuche oder zur Energiegenerierung, d.h. das oben erläuterte Smart Metering. Das HAN entspricht dem Smart Home, zumindest soweit es sich um im Sinne des Smart Grid steuerbare Geräte handelt (CLS). Weiterhin rechnet die Richtlinie die Endverbraucher- und die Serviceschnittstelle hier hinzu. Das WAN bietet die Verbindungen zum Smart Grid mit den verschiedenen Akteuren, hier Externe Marktteilnehmer (EMT) genannt. Neu ist in diesem Kontext die Rolle des Smart Metering Gateway Administrators. Nur er darf das SMGW „aufwecken“ und so eine Kontaktaufnahme seitens des SMGW initiieren. Generell sieht das Sicherheitskonzept vor, dass alle Verbindungsaufnahmen ins WAN nur durch das SMGW erfolgen. Auch Um- und Neukonfiguration muss über den SMGW Administrator erfolgen. Neu ist in der TR-03109 auch das Sicherheitsmodul, das verschiedene Sicherheits- und Kontrollaufgaben erfüllen muss. Dadurch entsteht auch eine weitere Schnittstelle, die zum Sicherheitsmodul. Hier kommen verschiedene kryptographische Verfahren und Kommunikationsmechanismen zum Einsatz.

Die Richtlinie macht zur Kommunikation im WAN (s. Abbildung 4) und im LMN (s. Abbildung 5) konkrete Aussagen. Für das HAN existieren vorrangig Kommunikationsprofile sowie Vorgaben zur Sicherheit.

Wie Abbildung 4 zeigt, sieht die Richtlinie DLMS/COSEM auf den oberen Kommunikationsebenen vor, das per HTTP über TCP/IP abgewickelt wird. Prinzipiell wird TLS (Transport Layer Security) verwendet, das die Verschlüsselung der Daten sicherstellt. Über CMS (Cryptographic Message Syntax) stehen Datenformate für die Inhaltsdatenverschlüsselung und -signatur zur Verfügung. Auf den untersten Schichten ist kein Übertragungsmedium vorgegeben, so dass hier alle üblichen Netzwerkkommunikationsimplementierungen möglich sind. Für Dienste neben dem eigentlichen Smart Metering und der SMGW-Administration sind auch weitere Protokolle erlaubt, die aber auf jeden Fall über TLS verschlüsselt kommunizieren müssen. Außer TCP/IP kann die Kommunikation auf der Transportschicht auch über weitere Protokolle erfolgen. TCP/IP dürfte aber in den meisten Fällen das Protokoll der Wahl sein.

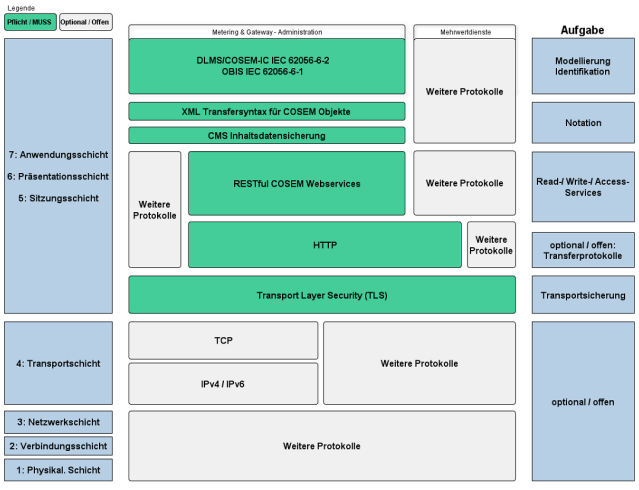

Abb. 4 Protokolle für die WAN-Kommunikation des SMGW [6]

Für den Bereich des LMN ist vorgeschrieben, dass das SMGW mindestens eine drahtgebundene und eine drahtlose Verbindung anbietet.

Für die fixe Verbindung schreibt die Richtlinie auf der Anwendungsebene OBIS und COSEM-Interfaceklassen vor mit den OBIS-Kennzahlen aus der DIN EN 13757-1 (M-Bus) vor. Darunter arbeitet SML über TLS. Auf den unteren Ebenen wird HDLC verwendet, das physikalisch über EIA/RS-485 symmetrisch kommuniziert.

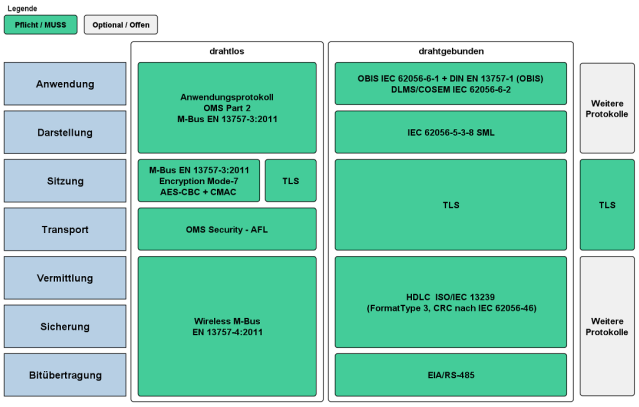

Abb. 5 Protokolle für die LMN-Kommunikation des SMGW [6]

Für die Funkverbindung schreibt die TR-03109 den M-Bus (EN 13757-3) mit einigen Einschränkungen vor. Da der Schutz durch die standardmäßige Verschlüsselung in der EN 13757-3 als nicht ausreichend erachtet wird, sieht sie eine spezielle Transportschicht (OMS Security Authentication and Fragmentation Layer (AFL) vor, die mit M-Bus Encryption Mode 7 gesichert sein muss. Die unteren Ebenen werden durch die Protokolle und Spezifikationen des wireless M-Bus (wM-Bus) abgedeckt. Weitere (Funk-) Protokolle können eingesetzt werden, sofern sie prinzipielle Sicherheitsvorgaben der TR erfüllen.

Die HAN-Schnittstelle muss mittels TLS gesichert sein und eine eindeutige Identifizierung und Authentifizierung ermöglichen. Sie muss über Ethernet (min. 10 MBit/s) mittels IP kommunizieren können. Weitere Protokolle sind möglich.

Praktische Untersuchungen

Neben den grundsätzlichen Untersuchungen zum Kommunikationsbedarfs eines „MUC Controllers“ alias Smart Metering Gateway waren auch exemplarische Implementationen vorgesehen.

Als Demonstrationsobjekt im LMN standen elektronische Zähler der Fa. Dr. Neuhaus (SMARTY ix-130, s. Abbildung 7) zur Verfügung, die die Vorgaben des VDE/FNN bezüglich Haushaltszählern erfüllen (eHZ, EDL21). Sie verfügen auch über einen eigenen MUC Controller (EDL40), der aber nicht genutzt wurde. Über diese Zähler wurden wechselnde Lasten betrieben, so dass reale Auslesedaten zur Verfügung standen. Um die Daten verarbeiten zu können, musste ein einfaches Interface realisiert werden. Damit war es möglich, die Zählerdaten über eine serielle Schnittstelle nach RS232 in den Rechner übernehmen zu können. In einem ersten Schritt erfolgte die Analyse der regelmäßig gelieferten Daten, die der Zähler im sog. Push Mode (selbsttätiges Senden ohne Aufforderung) lieferte. Die Informationen waren per SML codiert.

Abb. 7: EDL21-Zähler

Als Smart-Metering-Gateway-Ersatz fungierte ein normaler PC. Dieser nahm die Daten entgegen, prüfte sie und legte sie in passenden Datenstrukturen ab [11]. Der PC lief als Vorbereitung für eine passende Embedded Lösung unter Linux, so dass eine später erfolgte Portierung auf eine Embedded Hardware nur geringen Aufwand bedeutete. Zur Simulation der Kommunikation im Smart Grid wurde ein sog. Dummy Server auf einem weiteren PC (Linux) eingerichtet, der mit dem SMGW verbunden war [12]. Die gesamte Konfiguration zeigt Abbildung 8.

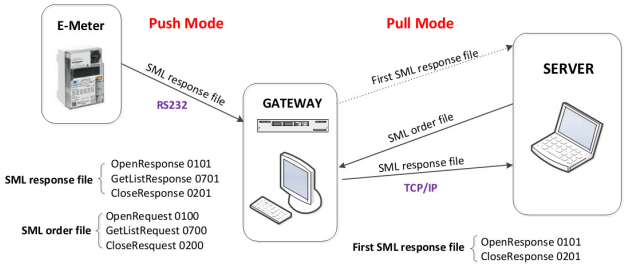

Abb. 8: Testkonfiguration [11]

Das Bild verdeutlicht auch die Betriebsarten der Kommunikation. Während der Zähler ständig Daten im Push Mode liefert, arbeitet das Gateway zum Server hin im sog. Pull Mode, d.h. er sendet Informationen nur auf Anfrage des Servers. Mittels entsprechender SML-Nachrichten wurde das Gateway aufgefordert, alle verfügbaren Daten oder gezielt ausgewählte Informationen an den Server zu senden. Dabei erfolgt die SML-Kommunikation über TCP/IP im Hochschulnetz. Um die Kommunikation zu starten, war es notwendig, mit den SML-Kommandos OpenResponse/Close Response die Verbindung einmalig zu initiieren. Die Anfrage nach Daten geschieht mittels GetListRequest, worauf das Gateway mit GetListResponse antwortet. Serverseitig wurden die Informationen in einer Datenbank abgelegt, aus der sie mittels einer einfachen Benutzeroberfläche abgefragt werden konnten.

Um die Kommunikation zwischen Zähler und SMGW bzw. zwischen diesem und dem Server zu implementieren, war es nötig, entsprechende SML-Protokollstacks zu nutzen. Das Gateway verwendete dafür die Bibliothek libSML, eine C-Implementation des Stacks. Der Server ist in Java realisiert, weshalb er mit einer anderen Bibliothek, der jSML (OpenMUC.org), arbeitet. Der Einsatz der Bibliotheken war nicht trivial, da sie noch fehlerhafte Softwareteile enthielten.

Um auch weitere Protokolle testweise einsetzen zu können, wurde die IEC 61850 zwischen SMGW und dem Server implementiert. Weiterhin erfolgten hierbei eine grundsätzliche Über-

arbeitung der Gateway-Implementierung und die oben schon erwähnte Portierung auf eine Embedded Hardware (s. Abbildung 9, ALIX Board, PCengines.ch). IEC 61850 verfolgt mit seiner Objektorientierung einen völlig anderen Ansatz als das doch recht simple SML. Nach anfänglichen Schwierigkeiten mit den Bibliotheken der openIEC61850 (OpenMUC.org) gelang aber auch hier die Kommunikation in der gleichen Konstellation wie unter SML.

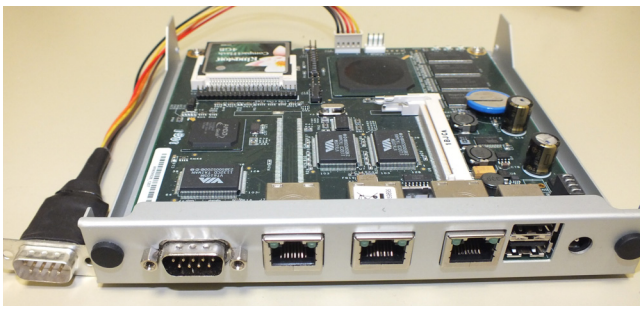

Abb. 9: ALIX Board, Basis für Embedded Implementierungen des SMGW

Der Server unterstützt jetzt den modellbasierten Ansatz der IEC 61850, während das Gateway zum Zähler hin per SML und in Richtung Server per IEC 61850 kommuniziert und die entsprechende Protokollumsetzung realisiert. Dabei wurde die Software so ausgelegt, dass sie dynamisch beim Anschluss weiterer Zähler neue Instanzen und Modelle für die IEC 61850 anlegt.

Ergebnisse

Im praktischen Teil des Projekts wurden auf Basis der gewonnen Informationen entsprechende Testsysteme implementiert, z.B. für die Kommunikation im Smart Metering mit SML sowie mit der IEC 61850. Dies zeigte, dass relevante Protokollstacks mit überschaubarem Aufwand für den praktischen Betrieb eingesetzt werden können.

Insgesamt lieferte das Projekt einen guten Überblick darüber, welche Strukturen einerseits und welche Kommunikationsmechanismen andererseits derzeit vorgeschlagen und/oder sogar eingesetzt werden. Es wurde klar, wofür bereits genauere Empfehlungen und (Quasi-) Standards existieren und wo Lösungen eher proprietär und wenig universell nutzbar sind. Die zwischenzeitlich erschienene Technische Richtlinie des BSI gab hier in vielerlei Bereichen eine eindeutige Richtung vor. Allerdings stellt sich die Frage, wie sich das Smart Grid und das Smart Metering weiterentwickeln wird, insbesondere unter dem Aspekt, dass die Vorgaben nur für Deutschland gelten und sich eine Harmonisierung der Vorgehensweisen zumindest innerhalb Europas in keiner Weise abzeichnet.

Literatur

[1] BNetzA: *Smart Grid – Smart Market. Eckpunktepapier der Bundesnetzagentur zu den Aspekten des sich verändernden Energieversorgungssystems.* Bonn, 2011.

[2] ZVEI / BDEW: Smart Grids in Deutschland - Handlungsfelder für Verteilnetzbetreiber auf dem Weg zu intelligenten Netzen. Frankfurt/Berlin, 2012.

[3] Appelrath, H.-J. et al.: *Forschungsfragen im „Internet der Energie“*. acatech Materialien Nr. 1, München, 2011.

[4] Smart Grids European Technology Platform: *Strategic Deployment Document for Europe's Electricity Networks of the Future*. 2010. – www.smartgrids.eu

[5] FNN: *Lastenheft MUC – Multi Utility Communication Version 1.01 - 04. Juli 2011 [Arbeitsfassung]*. VDE, Frankfurt, 2011.

[6] BSI: *Technische Richtlinie BSI TR-03109*. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[7] De Craemer K., Deconinck G.: "Analysis of State-of-the-art Smart Metering Communication Standards," YRS edition, Leuven, Belgium, p. 29-30, 2010.

[8] BSI: *Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073)*. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[9] BSI: *Schutzprofil für das Sicherheitsmodul eines Smart Meter Gateways (BSI-CC-PP-0077)*. Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2013.

[10] PTB: *PTB-A 50.7 Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme*. Physikalisch-Technische Bundesanstalt. Braunschweig, 2004.

[11] He, B.: *Development and Implementation of a SML-based Communication Concept for a Smart Metering Gateway*. Bachelorarbeit. Ostfalia Hochschule für angewandte Wissenschaften, Wolfenbüttel, 2012.

[12] Li, Q.: *Development and Implementation of a SML-based Communication Concept for a Smart Metering Server*. Bachelorarbeit. Ostfalia Hochschule für angewandte Wissenschaften, Wolfenbüttel, 2012.

Kontaktdaten

Ostfalia Hochschule für angewandte Wissenschaften
Fakultät Elektrotechnik
Prof. Dr.-Ing. Rainer Bermbach
Salzdahlumer Straße 46/48
38302 Wolfenbüttel
Telefon: +49 (0)5331 939 42620
E-Mail: r.bermbach@ostfalia.de
Internet: www.ostfalia.de/pws/bermbach