



## Kommunikationsinfrastruktur für Smart Metering

Sven Müller, Sebastian Trampler, Georg Jung

### Zusammenfassung

Das Projekt *Smart Grid Solar* ([www.smart-grid-solar.de](http://www.smart-grid-solar.de)) erforscht die Möglichkeiten zur substantiellen Erhöhung des Anteils von lokal gewonnenen erneuerbaren Energien (EE) – insbesondere Photovoltaik – am Primärenergiemix in Niederspannungsnetzen.

Die verschiedenen Mess-, Erzeuger-, und Speicherkomponenten der Teilprojekte sind geographisch in Arzberg und Hof unregelmäßig verteilt und größtenteils nicht leicht zugänglich. Die an den Messstationen erhobenen Daten müssen zeitnah und zuverlässig zentral gesammelt werden, um den Projektpartnern strukturiert zur Verfügung zu stehen.

### 1 Auslegung der Kommunikationsinfrastruktur am Beispiel der Ortsnetzmessung

Insbesondere die präzise Erfassung der elektrischen Größen innerhalb des Ortsnetzes in zeitlich hoher Auflösung erfordert nach heutigem Stand der Planung Messeinheiten in mindestens 50 verschiedenen Haushalten und/oder Netzknoten. Die maximal erreichbare zeitliche Auflösung und die größtmögliche Genauigkeit der zu erfassenden Werte ist dabei zunächst durch die verwendeten Messinstrumente begrenzt. Weiterhin beschränken die Notwendigkeit der Übertragung der gemessenen Werte die erreichbare Auflösung. Diese hängt wiederum vom jeweils lokal zur Verfügung stehenden Pufferspeicher sowie vom Kommunikationskanal, den verwendeten Protokollen und den Anforderungen an Datensicherheit ab. Unter diesen Bedingungen muss nun der ideale Einsatz der Ressourcen ermittelt werden.

Eingehend betrachtet wurden in diesem Zusammenhang bisher die Geräte der Firma EMH Metering bei einem Treffen mit einem Firmenvertreter am 16.12.2013 am ZAE in Erlangen gemeinsam mit den Projektpartnern aus Arbeitspaket 1.1 – Netzmanagement. In Folge stellte EMH zwei Geräte vom Typ LZQJ-XC mit je einem VARIOMOD-XC Kommunikationsmodul sowie Konfigurations- und Treibersoftware zur Verfügung. Diese werden zur Zeit (Seit dem 7.1.2014) sowohl im Paket 0.1 als auch im Paket 1.1 näher untersucht (Anmerkung: Im Livebetrieb sollen alle Geräte mit Mobilfunk-Modulen ausgestattet werden).

Die Geräte, deren Elektronik auf Smart Metering Aufgaben ausgelegt sind (also auf ein wesentlich gröberes Zeitraster), sind nach bisherigem Stand durchaus in der Lage in ausreichender zeitlicher Auflösung Daten zu erfassen und in internen Registern abzulegen. Zur Kommunikation der Daten nach außen steht aber nur eine relativ langsame serielle Schnittstelle

---

#### Kontakt

[georg.jung@iisys.de](mailto:georg.jung@iisys.de)  
[www.iisys.de/sg](http://www.iisys.de/sg)  
+49 9281 409-6271  
+49 9281 409-55-6271 (fax)

Alfons-Goppel-Platz 1  
95028 Hof/Germany  
phone +49 9281 409-6112

[info@iisys.de](mailto:info@iisys.de)  
[www.iisys.de](http://www.iisys.de)

zur Verfügung. Die erste Optimierungsaufgabe läge also hier in der Erstellung eines oder mehrerer geeigneter Vektoren von Messgrößen die einen guten Kompromiss zwischen zeitlicher Auflösung und Datenmenge und -art darstellen.

Zur Überbrückung der räumlichen Distanz stehen mehrere Kommunikationstechnologien zur Verfügung, wobei die Kosten der jeweiligen Lösung die für die Messgeräte selbst zur Verfügung stehenden Ressourcen einschränken, in der Optimierung also nicht unabhängig gesehen werden können. Die Aufgabe zerfällt in zwei Teile, die Auswahl eines oder mehrerer geeigneter Übertragungsprotokolle sowie die Auswahl des Übertragungsmediums.

Als Medien werden zur Zeit Mobilfunk (GMS, GPRS), Kabel, Power-line-communication (PLC) sowohl in Schmalband- als auch in Breitbandtechnologie, und DSL Lösungen betrachtet. Dabei gab es den folgenden technischen Vergleich der Kommunikationsmöglichkeiten (Medium, Protokoll) verschiedener Anbieter von (Mess- und) Kommunikationstechnik (Anmerkung : Es erfolgte eine Vorauswahl durch AP 1.1, um die messtechnischen Anforderungen sicherzustellen.)

- Power Plus Communications (Breitband PLC)
- ENTES Elektronik (Ethernet, Mobilfunk)
- PCE Deutschland GmbH (Ethernet, Mobilfunk)
- Landis+Gyr (Ethernet, Mobilfunk)
- EMH metering GmbH&Co. KG (Ethernet, Mobilfunk)

Es ergibt sich folgendes Bild

- Mobilfunk. Für die stationären Messstationen ist auf ortsungebundene Kommunikation ausgelegter Mobilfunk zunächst nicht naheliegend. Zwar wäre keine Neuverlegung von Kabeln oder Einrichtung von Anschlüssen notwendig, gewöhnliche Mobilfunklösungen im Endanwendermarkt sind aber kostenintensiv und ausfallgefährdet, zudem lässt sich die Aufstellung der Messgeräte nicht immer günstig mit Blick auf die Funkanbindung einrichten. Allerdings stehen gerade im Metering-Bereich Lösungen zur Verfügung, die durch Großkundenverträge kostengünstig sind, und durch Bündelung mehrerer Netze eine hohe Ausfallsicherheit gewähren. Diese Möglichkeiten werden zur Zeit untersucht.
- Kabel. Kabelverträge wurden noch nicht eingehend betrachtet. Diese sind gewöhnlich auf sehr hohe Datenraten ausgelegt und für die Übertragung von Messdaten überdimensioniert.
- PLC. Power-line-communication wurde mit verschiedenen Anbietern diskutiert und Erfahrungen Dritter wurden ausgewertet. Insgesamt bietet sich ein durchwachsenes Bild. Bei ausreichender Knotendichte scheinen insbesondere Breitbandlösungen gut zu funktionieren, allerdings zeigen sich häufig Probleme mit der Saklierbarkeit sowie gegenseitige Störungen mit Radiowellenkommunikation. Da die Untersuchung der Kommunikationskanäle nicht im Vordergrund steht, sehen wir zur Zeit von solchen Lösungen ab.
- DSL. Im DSL-Bereich stehen auf dem Markt Lösungen mit geringen Datenraten kostengünstig zur Verfügung. Solche Lösungen bedeuten vor allem organisatorisch einen hohen Aufwand.

Auf Protokollseite wurden bisher die Standards IEC62056, DLMS/COSEM, SML und M-Bus untersucht, bei allen handelt es sich um etablierte Industriestandards, die Auswahl wird letztenendes durch die Wahl der Messinstrumente bestimmt (das untersuchte Messgerät LZQJ-XC bietet als Kommunikationsprotokoll DLMS/COSEM).

## 2 Vertraulichkeit, Integrität und Verfügbarkeit der Daten

Zur Sicherheit der Datenübertragung existieren die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die einschlägigen Verordnungen für Smart Metering (BSI TR-03109, siehe auch BDEW Whitepaper Empfehlung: Anforderung an sichere Steuerungs- und Telekommunikationssysteme) lassen sich im Projekt nach derzeitigen Stand nicht mit vertretbarem Aufwand implementieren. Teilweise steht geforderte Hardware (Hardwareimplementierte Kryptographie, speziell für Verschlüsselung durch elliptische Kurven) nicht zur Verfügung, teilweise sind die Anforderungen im Detail zumindest dort wo keine Steueraufgaben übernommen werden, für die Größenordnung des Projekts schlicht überdimensioniert. Beispielsweise ist die Angreifbarkeit von Verschlüsselung auf der Grundlage qualitativ minderwertigen (Software-implementierten) Pseudozufallszahlengeneratoren mit statistischen Methoden für die zu erwartenden Datenmengen schlicht zu aufwändig, die daraus resultierende Gefahr für die Vertraulichkeit der Daten im Vergleich zu anderen Faktoren schätzen wir als vernachlässigbar ein. Rechtlich gesehen ist die Umsetzung der BSI Verordnungen zunächst nicht notwendig, da, einschließlich eingeräumter Übergangszeiträume, die Regelungen erst nach Projektabschluss verbindlich sind.

Leider besteht bei der Nutzung von am Markt erhältlichen Mobilfunkmodulen für Smart Meters noch nicht einmal die Möglichkeit zu Software-implementierter Verschlüsselung, hier steht die erforderliche Rechenleistung an keiner Stelle der Kommunikationskette zur Verfügung. In diesem Fall sind die Daten in der Übertragung offen, und erst am Akkumulationspunkt (zentraler Server) geschützt.

Wichtiger als die Vertraulichkeit der von außerhalb des Projektes nur mit großem Aufwand zuzuordnenden und interpretierbaren Daten ist der Schutz der Integrität und Verfügbarkeit der Daten, Ausfälle durch DDOS oder durch Ausnutzung von Schwachstellen in der Netzanbindung (offene Ports, Scripting, *etc.*) bringen einem Angreifer zwar keine Vorteile, schädigen aber das Projekt.

Auf Datenbankseite werden die üblichen Mechanismen zur Nutzerauthentifizierung und Datensicherheit implementiert.