Wie wirkt das GNDEW auf Produktentwicklung –

Schwerpunkt: Digitalisierung von Systemen der Sektorenkopplung

Raimund Thiel, SMA Solar Technology AG für den
Bundesverband Solarwirtschaft

Raimund Thiel

25 Jahre @ SMA

Bereich:
Innovation Center & IP

Themen:
Smart Grids und Kommunikation

Raimund.Thiel@SMA.de

GNDEW

Ein lachendes und ein weinendes Auge

SMGW/GNDEW zusammengefasst

Digitaler Netzanschluss mit dem Netzanschlusspunkt (NAP) als Bezugspunkt, statt der Ansteuerung einzelner Komponenten wurde endlich anerkannt.

Möglichkeit zur 15minütigen Abrechnung und damit kostengünstige Möglichkeit zeitvariable Tarife zu realisieren.

Leistungsfähigkeit und langwierige Zertifizierungsprozesse des SMGW verhindern Innovationen.

Die Festlegung einer regulierten Technologie gefährdet erprobte Lösungen für ein zukünftiges SmartGrid, international bereits genutzte Lösungen werden weitgehend verhindert.

Bei Anlagensteuerung über iMSys sind Fragen ungeklärt, die aber für die Komponentenhersteller von entscheidender Bedeutung sind. (Es fehlt z.B. noch die BSI-TR-03109-5 – Anschluss von Geräten im Kundennetzwerk unklar).

Übersicht

- GNDEW und Realität –
  Herausforderung: Anbindung an Kundennetzwerk
- Problemstellung Cyber-Sicherheit
  TR03109 und Protection Profile
- Rahmenbedingungen/deutsche Besonderheiten
  Herausforderung: energiewirtschaftlich relevante Daten
- Ausblick

GNDEW wird der Realität nicht überall gerecht

- Deutlicher Fortschritt für Abrechnung und Bilanzierung.
- Beim Thema „Steuern“ Verbesserungen aber auch offene Fragen (Bisherige Angebote „entwertet“?)
- Nationale Sonderlösung

- Teilweise Geänderte Betriebskonzepte notwendig
- Neue Schnittstellen/Protokolle
- Zusätzliche Kosten auch für kleine EE-Anlagen da verpflichtende Funktionen als „Zusatzleistung“ deklariert sind

Interaktionen mit der Liegenschaft - Stakeholder

Standardisierung

In der Standardisierung werden unterschiedliche Kommunikationsstandards (national und international) beschrieben.

Netzbetreiber

Die Rahmendbedingungen für den Netzanschluss werden in den technischen Anschlussbedingungen innnerhalb des gültigen Rechtsrahmens festgelegt.

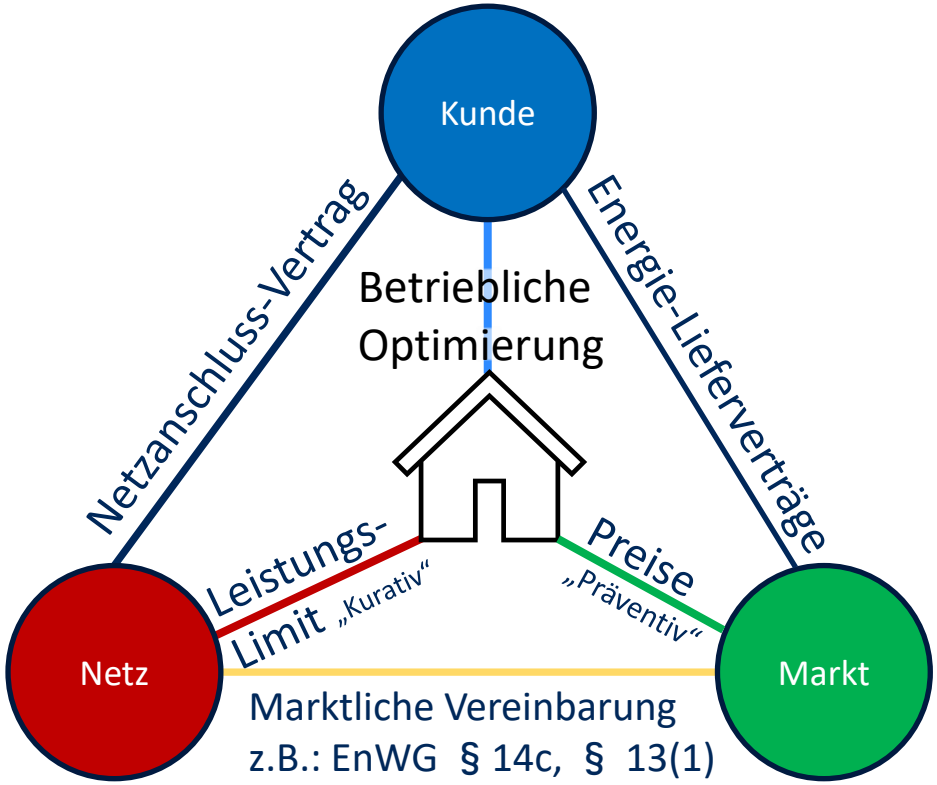
Liegenschaft

Die Anlage und deren Betrieb liegt in der Verantwortung und unter der Hoheit des Betreibers.
Es sind die jeweils national/regional gültigen Rahmenbedingungen zu beachten.

Cyber-Security

In internationalen Standards (z.B.: IEC 62443) werden Standards für die Informationssicherheit festgelegt. Zusätzlich gibt es regulatorische Vorgaben (z.B: EU Cyber Security Act) und zusätzlich nationale Besonderheiten

Interaktion mit der Liegenschaft - Beziehungen

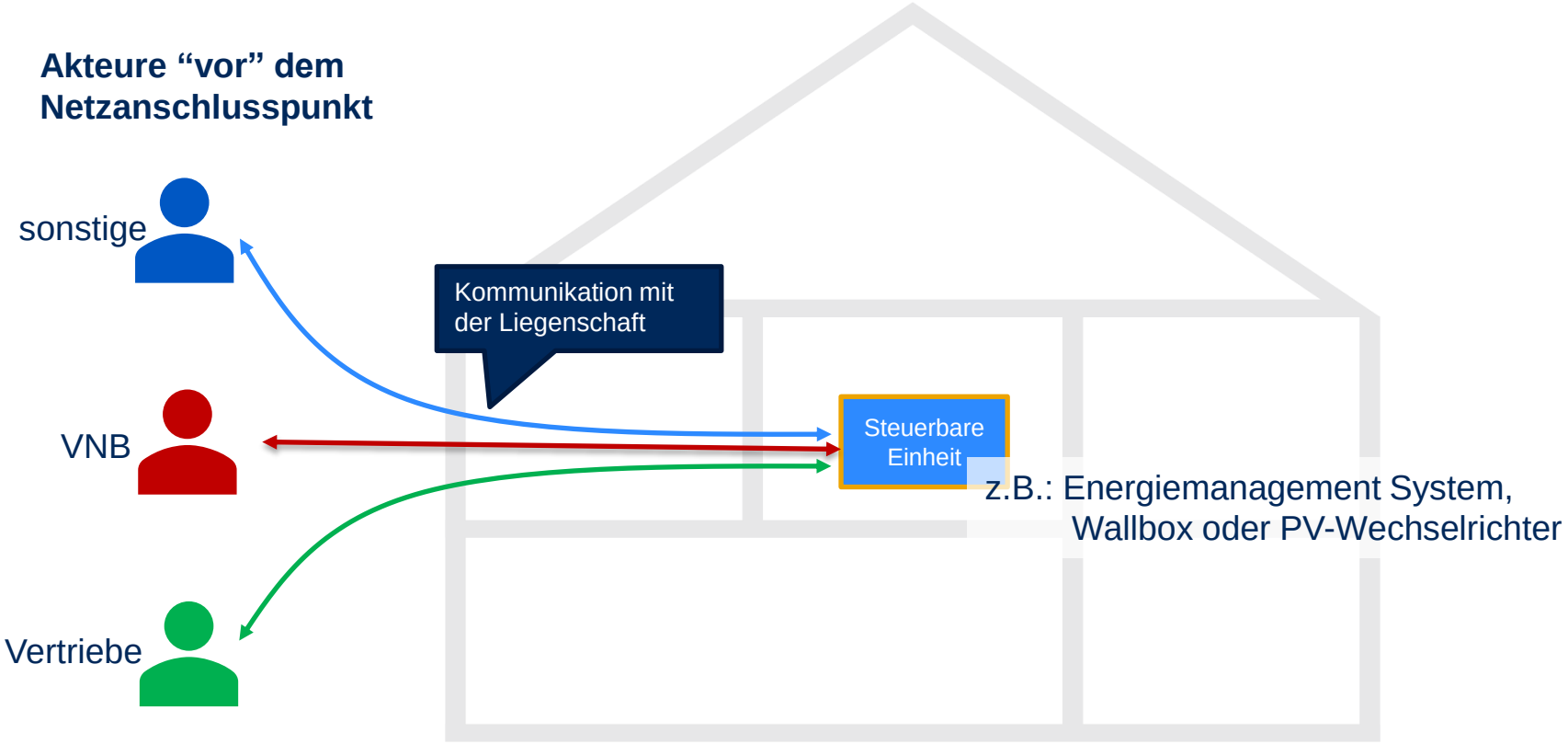


Umfeldbetrachtung konkret

Integration der erfolgten Digitalisierung

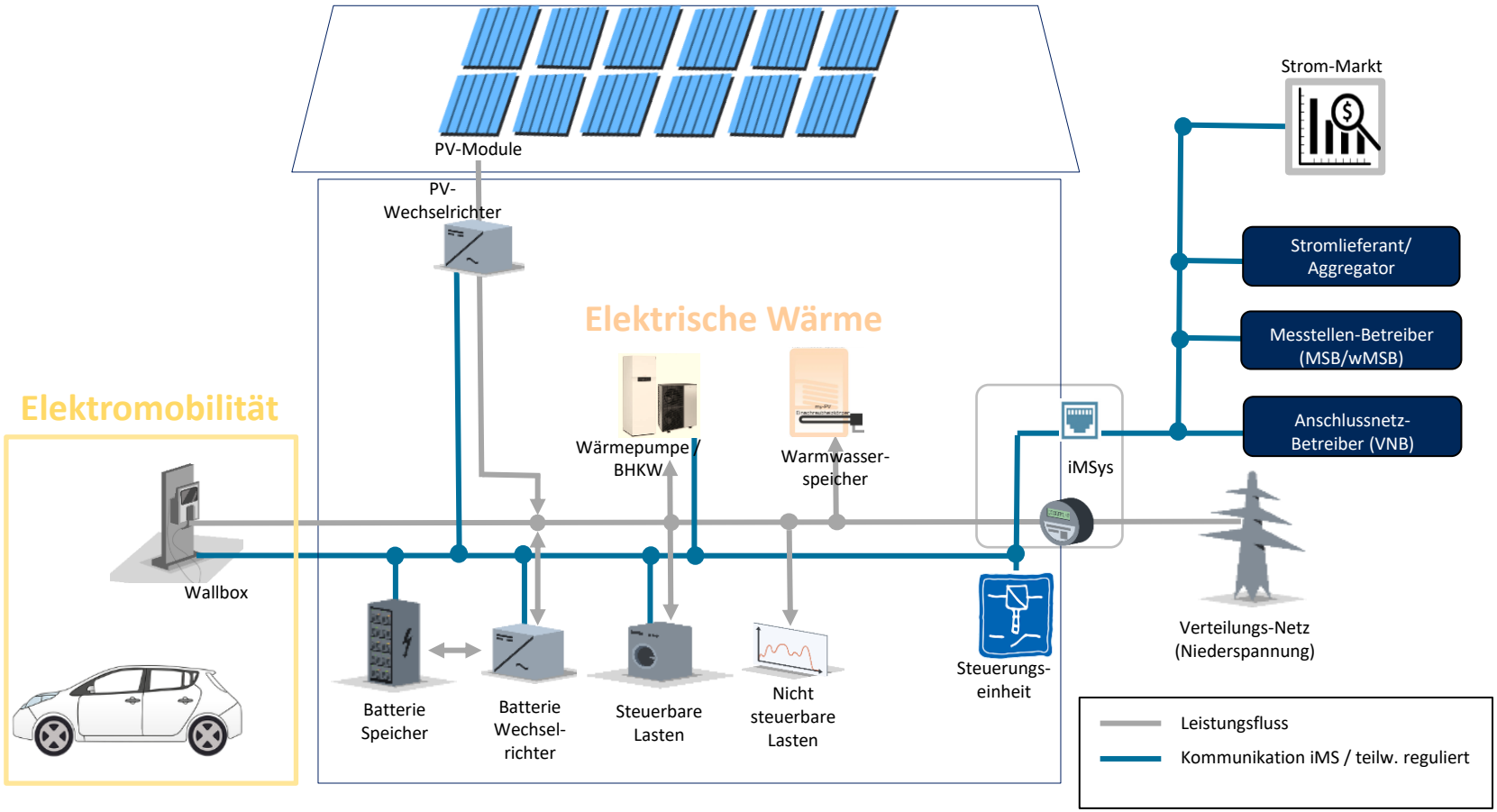
Interaktion mit der Liegenschaft - Systembild

Akteure “vor” dem Netzanschlusspunkt



Smartmeter-Gateway mit HAN-CLS

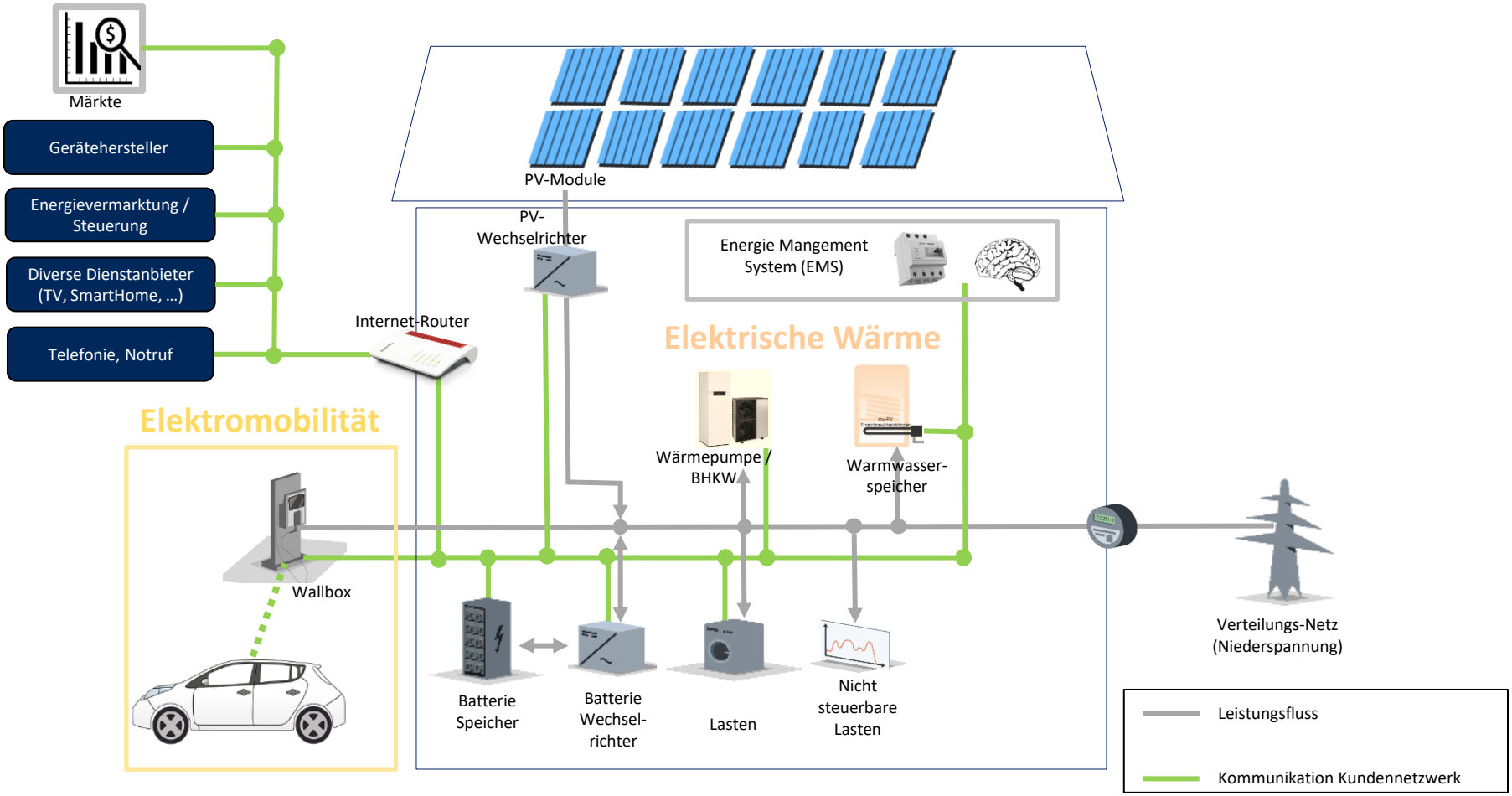
- Idee zur Digitalisierung des (Energie-)Systems



Anlagensteuerung über CLS im HAN

Die Welt heute – Status Quo

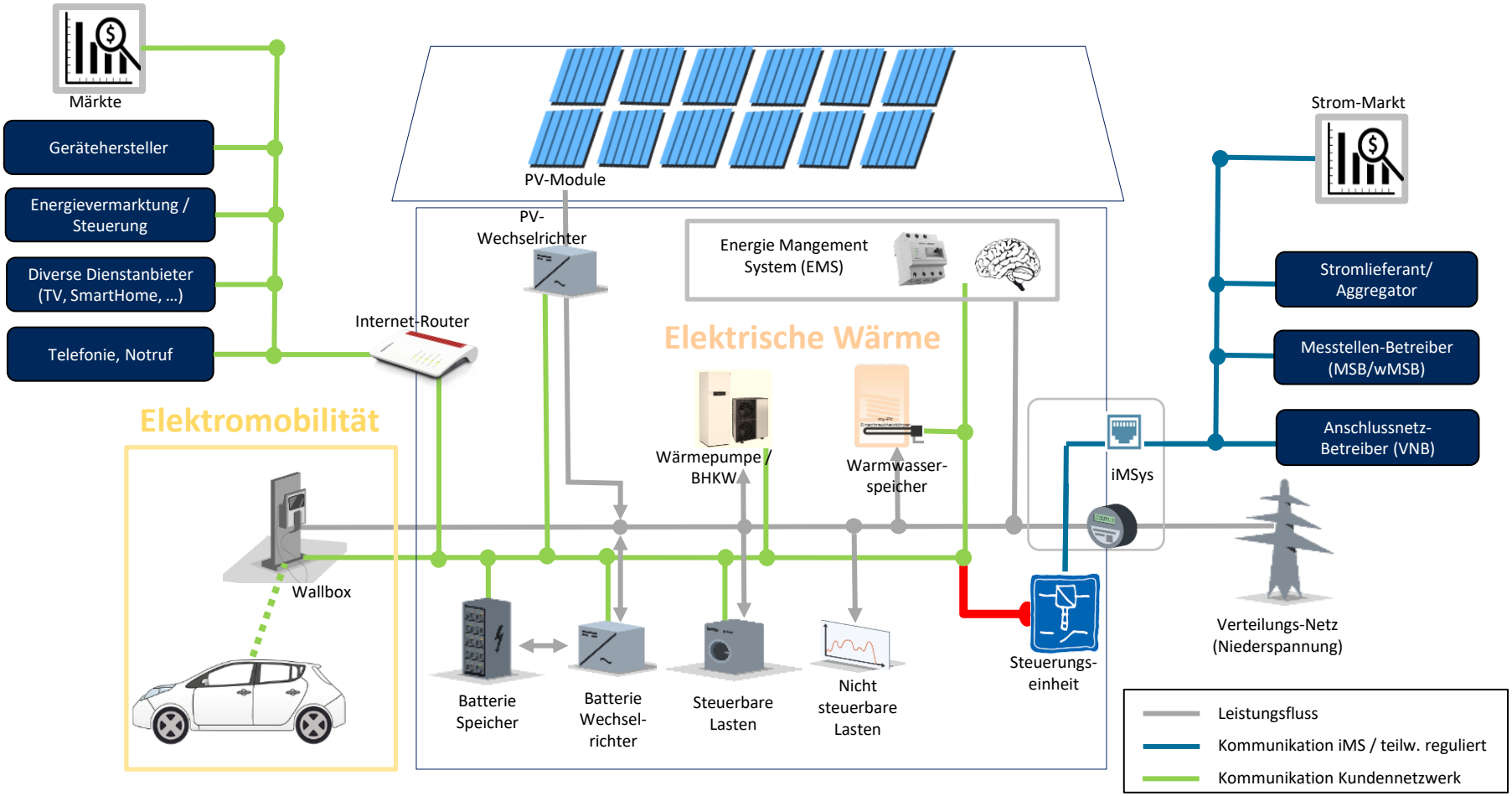
- Kommunikation im Wettbewerbsumfeld (auch international)



Problemstellung: Verbindung mit vorhandenem Kundennetzwerk

Smartmeter-Gateway im Gesamtkontext

- Sektorenkopplung in einer bereits digitalisierten Umgebung



Problemstellung: Verbindung mit vorhandenem Kundennetzwerk

Fragen zur Digitalisierung der Liegenschaft

- Wie kann die Verbindung zwischen Komponenten des intelligenten Messsystems und Netzwerk der Anlage/Liegenschaft praktikabel realisiert werden?
- Sind dem Installateur grundsätzlich Eingriffe in das Kundennetzwerk erlaubt?
- Was sind die Anforderungen an die Zuverlässigkeit/Verfügbarkeit des Kundennetzwerks?
- Kann der MSB (wMSB), der eine Steuereinheit installiert auch die Verbindung zu Geräten im Kundennetzwerk herstellen?
  - Was passiert bei Änderungen im Kundennetzwerk („FritzBox,-Tausch“)

Aspekte einer zeitgemäßen Digitalisierung

- Offene Schnittstelle ins Internet zwingend erforderlich für moderne Dienstleistungen und Geschäftsmodelle.
- Es muss praktikabel sein, die Verbindung zwischen Komponenten des intelligenten Messsystems und dem lokalen digitalen Netzwerk der Anlage/Liegenschaft herzustellen.
- behördliche Zertifizierung von „allen“ Geräten (Wechselrichter, Batterien, Wärmepumpen etc.) muss durch eine Herstellererklärung ersetzt werden.
- Lösungen müssen *international nutzbar* sein – rein deutsche Lösungen sind nicht akzeptabel und schwächen die internationale Wettbewerbsfähigkeit.

Hintergründe – Problematik Cybersicherheit

BSI-CC-PP-0073 „Schutzprofil für das Smart-Meter-Gateway“

BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb

BSI-CC-PP-0073
protection profile zur TR 03109

O.Firewall The TOE shall serve as the connection point for the connected devices within the LAN to external entities within the WAN and shall provide firewall functionality in order to protect the devices of the LMN and HAN (as long as they use the Gateway) and itself against threats from the WAN side.

The firewall:

- shall allow only connections established from HAN or the TOE itself to the WAN (i.e. from devices in the HAN to external entities in the WAN or from the TOE itself to external entities in the WAN),
- shall provide a wake-up service on the WAN side interface,
- shall not allow connections from the LMN to the WAN,
- shall not allow any other services being offered on the WAN side interface,
- shall not allow connections from the WAN to the LAN or to the TOE itself,
- shall enforce communication flows by allowing traffic from CLS in the HAN to the WAN only if confidentiality-protected and integrity-protected and if endpoints are authenticated.

For communications within the different networks the following assumptions are defined:

1. Communications within the **WAN** are not restricted. However, the Gateway is not involved in this communication,
2. No communications between devices in the **LMN** are assumed. Devices in the LMN may only communicate to the Gateway and shall not be connected to any other network,
3. Devices in the **HAN** may communicate with each other. However, the Gateway is not involved in this communication. If devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is assumed to be appropriately protected. It should be noted that for the case that a TOE connects to more than one HAN communications between devices within different HAN via the TOE are only allowed if explicitly configured by a Gateway Administrator.

OE.Network It shall be ensured that

- a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,
- the Gateway is the only communication gateway for Meters in the LMN,
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

HAN, Home Area Network	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes.	[CEN], adopted
LAN, Local Area Network	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this PP the term LAN is used as a hypernym for HAN and LMN.	[CEN], adopted

OE.PhysicalProtection The TOE shall be installed in a non-public environment within the premises of the consumer that provides a basic level of physical protection. This protection shall cover the TOE, the Meters that the TOE communicates with and the communication channel between the TOE and its Security Module. Only authorised individuals may physically access the TOE.

Folgerungen aus BSI-CC-PP-0073

- Es wird angenommen, dass die Kommunikation im HAN über „andere“ Schnittstellen über ein passendes Sicherheitsniveau verfügt.
- Das kann bisher nicht für alle Geräte im LAN des Kunden (LAN<>HAN) sichergestellt werden.
- Daraus folgt, dass die geforderten Annahmen des PP nicht erfüllt wären, was die Zertifizierung der Gateways grundsätzlich in Frage stellen würde.
- Verhindert man jegliche „andere“ Kommunikation, so ist das Sicherheitsniveau von „*keine Kommunikation*“ sehr hoch.

→ die noch ausstehende BSI TR-03109-5 *kann* das Problem auflösen

  – „Bei der Technischen Richtlinie BSI-TR-03109-5 für das Themengebiet "Anforderungen an weitere Systemeinheiten des intelligenten Messsystems" handelt es sich derzeit um einen Platzhalter. Die Erstellung bzw. Publikation dieser Richtlinie ist in Planung.“

GNDEW und BNetzA

Energiewirtschaftlich relevante Daten (ERD)

Historie – ERD* bei BNetzA

Bundesnetzagentur
Beschlusskammer 6

Bundesnetzagentur
Beschlusskammer 7

BK6-22-253

Positionspapier

zur Konkretisierung der Reichweite energiewirtschaftlich relevanter Mess- und Steuerungsvorgänge nach § 19 Absatz 2 MsbG

...

Allerdings unterliegen nach Überzeugung der Beschlusskammern auch alle von einem Dritten initiierten Steuerungsvorgänge von Dritten (u.B. Lieferanten, Direktvermarktungsunternehmen oder Aggregatoren) aufgrund der mit einer Aggregation von Steuersignalen einhergehenden Gefahr der Herbeiführen netzkritischer Situationen einer Einordnung als ERD. Dies umfasst sowohl direkte als auch mittelbare Steuersignale, wie z.B. Preissignale, die in den Systemen des Anschlussnutzers/Anschlussnehmers als Auslöser einer Steuerungshandlung hinterlegt sein könnten.

...

*ERD = **E**nergiewirtschaftlich **r**elevante **D**aten

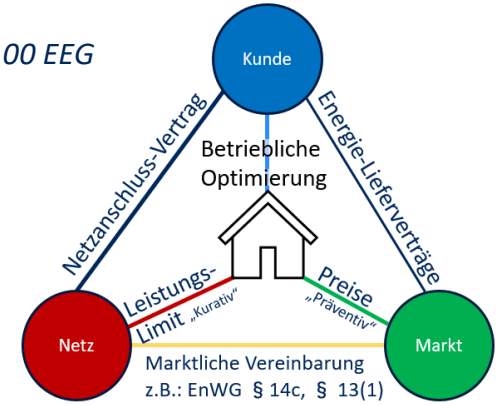
Hintergründe - GNDEW zu ERD* im MsbG

§ 19 Allgemeine Anforderungen an Messsystem

(2) Zur Datenverarbeitung *energiewirtschaftlich relevanter Mess- und Steuerungsvorgänge* dürfen *ausschließlich* solche technischen Systeme und Bestandteile eingesetzt werden, die den Anforderungen aus den § § 21 und 22 genügen. Energiewirtschaftlich relevante Mess- und Steuerungsvorgänge sind abrechnungs-, bilanzierungs- oder netzrelevante Standard- und *Zusatzleistungen nach § 34, insbesondere Standardleistungen nach § 34 Absatz 1 Nummer 1, 2, 4 und 5 sowie Zusatzleistungen nach § 34 Absatz 2 Satz 2 Nummer 2 bis 5 und 8, 9 und 11.*

- *§ 34 Absatz 1 unkritisch, nur Zählerstände, ggf. Problem wenn nur über SMGW (APPs etc…)*
- *§ 34 Absatz 2 2. Steuerung nach §14a EnWG (Hüllkurve)*
- *§ 34 Absatz 2 3. § 13a EnWG : Redispatch (steuerbare ohne Leistungsgrenze!)*
- *§ 34 Absatz 2 4. Direktvermarktung und § 14 c EnWG (Flexibilitätsdienstleistungen)*
- *§ 34 Absatz 2 5. Ist-Einspeisung und stufenlose Fernsteuerung sowie Anlagen nach § 100 EEG*

- *§ 34 Absatz 2 8. ab 2028 die Teilnahme am Regelenergiemarkt*
- *§ 34 Absatz 2 9. minütliche Netzzustandsdaten - unkritisch*
- *§ 34 Absatz 2 11. schwarzfallfeste dedizierte Weitverkehrsverbindung nach Maßgabe BNetzA*



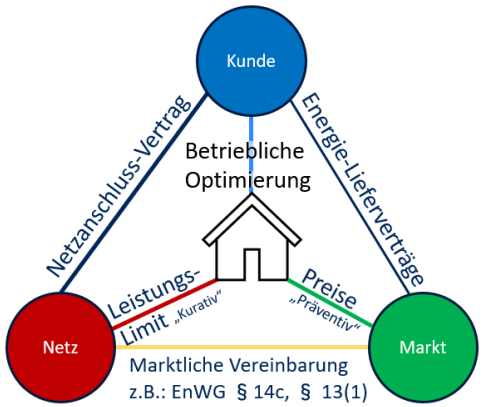
*ERD = Energiewirtschaftlich relev

Fragestellungen – Energiewirtschaftlich relevante Daten

Leistungen nach 13a , 14a, 14c EnWG und Direktvermarktung nach EEG oder KWKG müssen über Smart Meter Gateway kommuniziert werden.

Sonstige Steuerungen ebenfalls?

- → Umgang mit bisherigen Lösungen?
  - → Apps, virtuelle Kraftwerke, Pooling von Kleinanlagen, …
- → Kostentragung bei höheren Kosten gegenüber bisherigen Lösungen?
- → Leistungsfähigkeit, Verfügbarkeit, etc. im Vergleich zu bisherigen Lösungen?
- → Innovationsgeschwindigkeit (Technologieoffenheit)?



Fazit und Ausblick

Schön wäre…

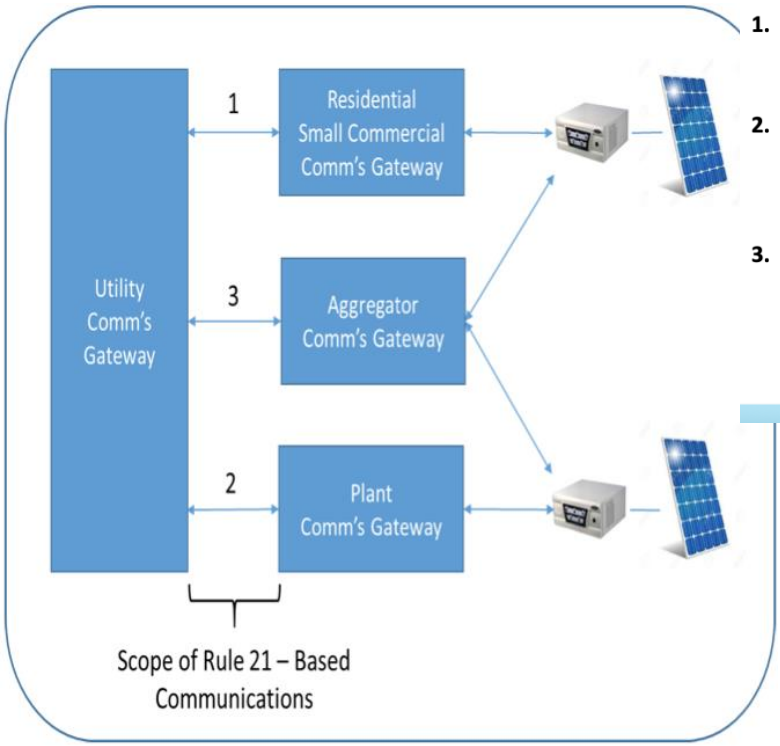
Gateway Regulierung auf Messung und Bilanzierung beschränken

- Die Steuerung von Anlagen über das SMGW ist zukünftig technisch denkbar, aber sollte sich im Wettbewerb mit anderen IT-Systemen behaupten.
  - Wo Steuerung benötigt wird, wird sie heute auch ohne Smart Meter Gateway umgesetzt.
- Die wirklichen Kosten für die Nutzung des CLS-Kanal sind für „Zusatzleistungen“ noch nicht absehbar. Was ist zum Beispiel mit virtuellen Kraftwerken, die im Sekundentakt kommunizieren/regeln?
- Messen und Bilanzieren über SMGW wird für Geschäftsmodelle benötigt und eingesetzt.

Verzicht auf Pflicht zum Steuern über iMSys für marktliche Anwendungen:

- Rechtssicherheit für SMGW bei modernen Geschäftsmodellen.
- Technologieoffener Ansatz ermöglicht hohe Innovationsgeschwindigkeit
- Wettbewerbliche Motivation zur Nutzung eines SMGW bei passendem Preis-/Leistungsverhältnis

Vielen Dank
für Ihre Aufmerksamkeit



1. **Direct** – Inverter directly communicates with the Utility Server
2. **EMS-Gateway** – Entity/Device that manages a small number of local Inverters.
3. **Aggregator** – Entity that manages communications for a fleet of Inverters. Assumed to be a cloud-based Server. This is the utility's preferred model of operation.

1. Direkt: Erzeugungsanlage kommuniziert direkt mit der Leitsystem-Anbindung
2. EMS Gateway – Ein Gerät, welches eine kleine Anzahl von lokalen Geräten verantwortet
3. Aggregator – Eine Funktionalität, die die Kommunikation zu einem „Schwarm“ von Geräten abbildet. *Das ist die bevorzugte Anbindung der „Utilities“ an den Betrieb*

Blick über den Tellerrand

Wettbewerbsfähige Lösungen international vorhanden

- In anderen Ländern wurden intelligente Lösungen über Backend eingeführt
- Cyber Security durch passende inter-nationale / nationale Standards an den relevanten Schnittstellen im Gesamtsystem