TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 23.05.2012

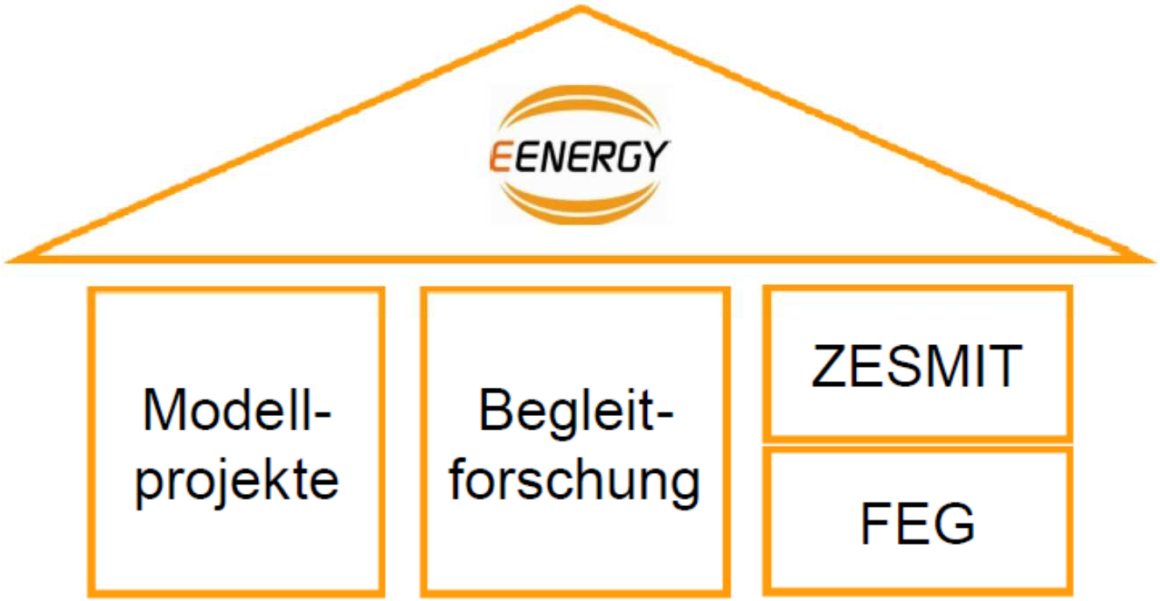
Wege zu einem sicheren SmartGrid
IKT-Förderaktivitäten des BMWi

Günter Seher, Projektträger im DLR
Christine Rosinger, OFFIS – Institut für Informatik

Inhalt

1. Überblick zu E-Energy
   - Modellregionen
   - Future Energy Grid
   - Studie Smart Grid Sicherheit
2. SecMobil
3. Smart Watts Sicherheitskonzept
4. Informationssicherheitsaspekte in eTelligence

1. E-Energy - E-Energy - IKT-basiertes Energiesystem der Zukunft



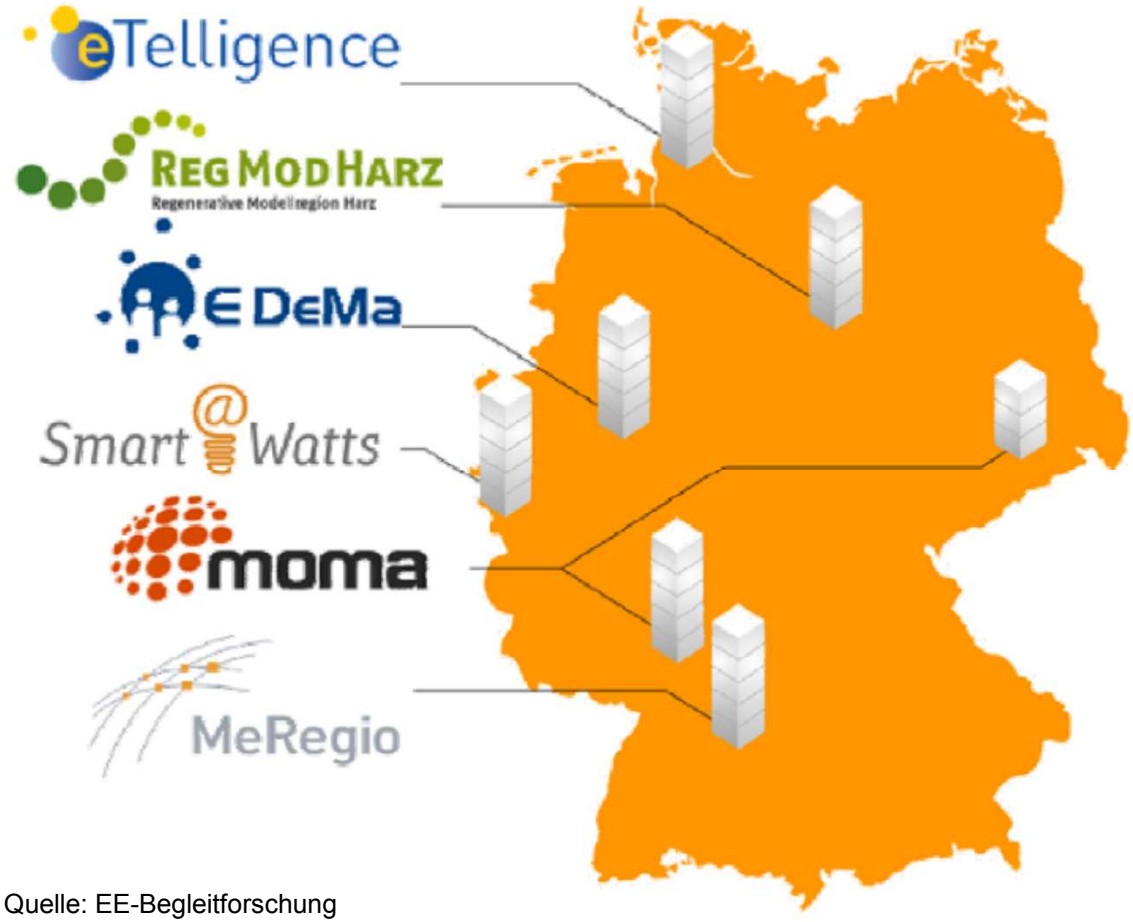
Quelle: EE-Begleitforschung

„Smart Grids made in Germany“

- F+E-Projekte 2008 - 2013
- 6 Modellregionen des BMWi und BMU
- Verschiedene Prototypen in Feldversuchen erprobt
- Begleitforschung und Studienprojekte ZESMIT und FEG
- Budget 140 Mio €, Förderung 60 Mio €

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
aufgrund eines Beschlusses des Deutschen Bundestages

1. E-Energy – Modellprojekte

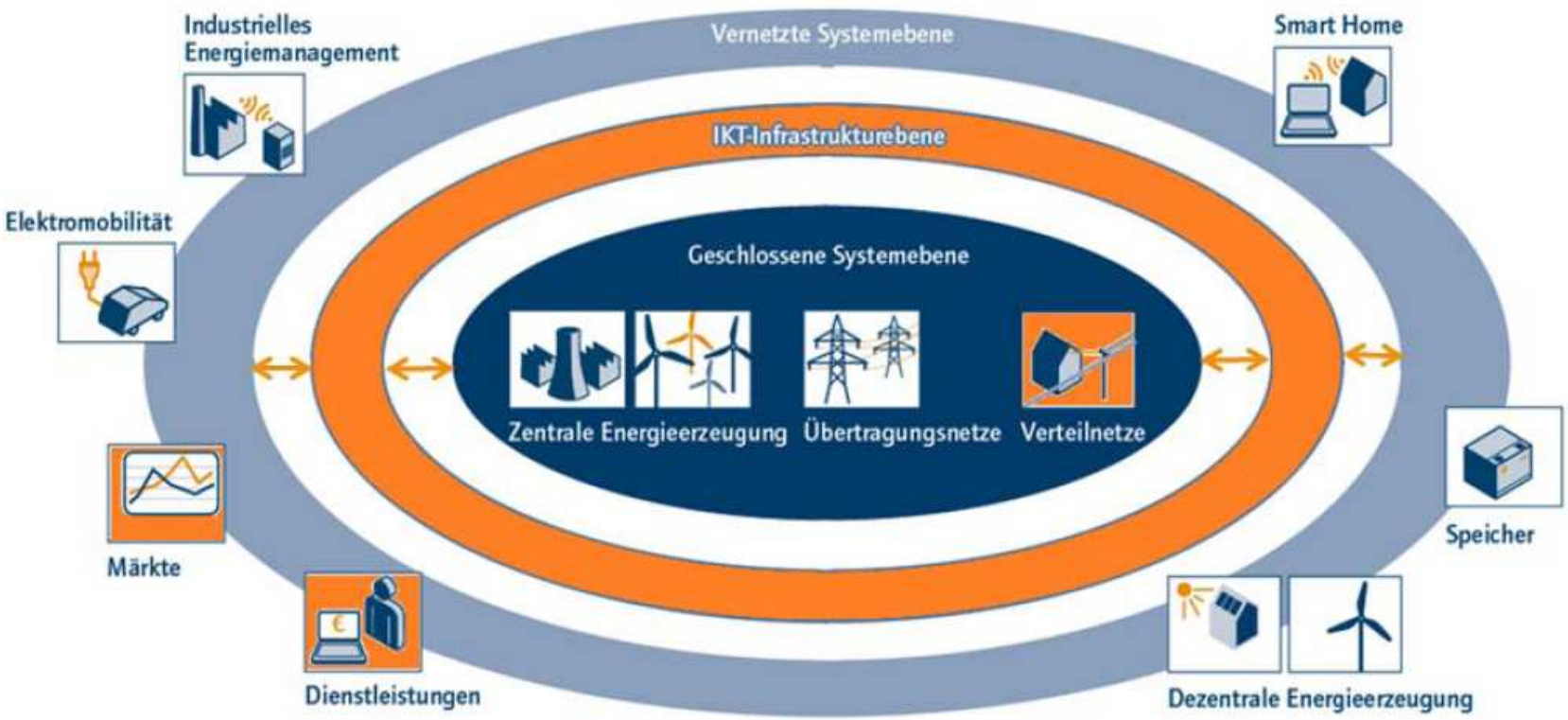


Quelle: EE-Begleitforschung

1. E-Energy – Multidimensionaler Forschungsansatz

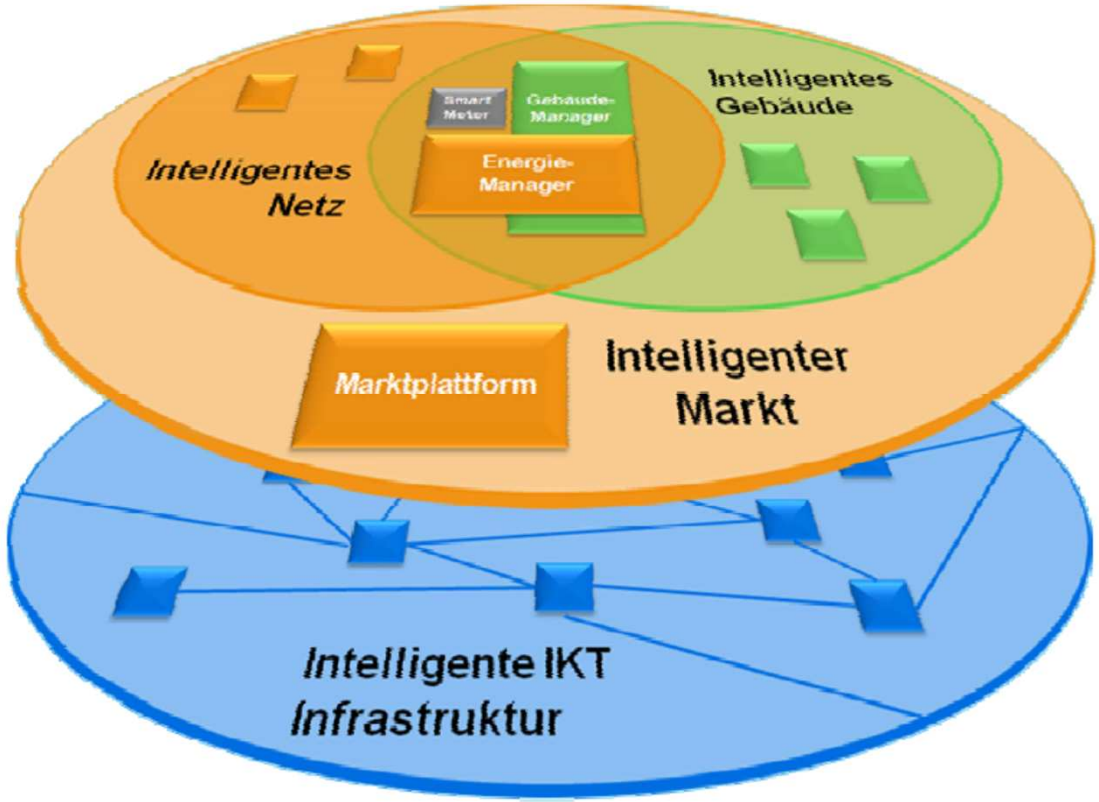
Quelle: EE-Begleitforschung

1. E-Energy – Systemkonzept



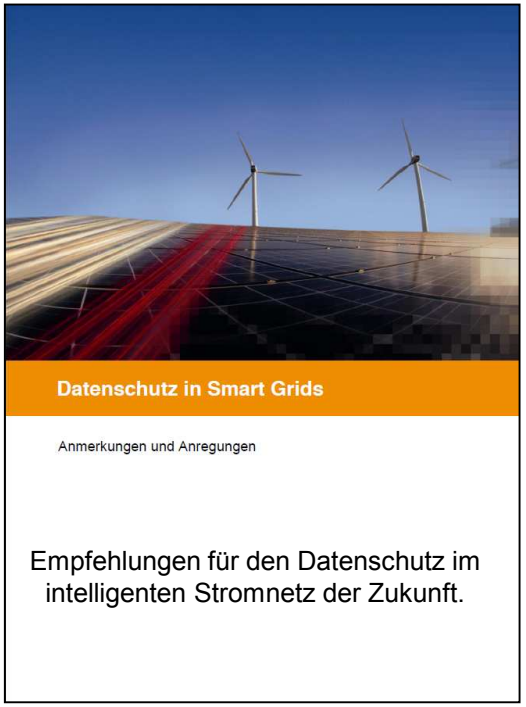
Quelle: EE-Begleitforschung

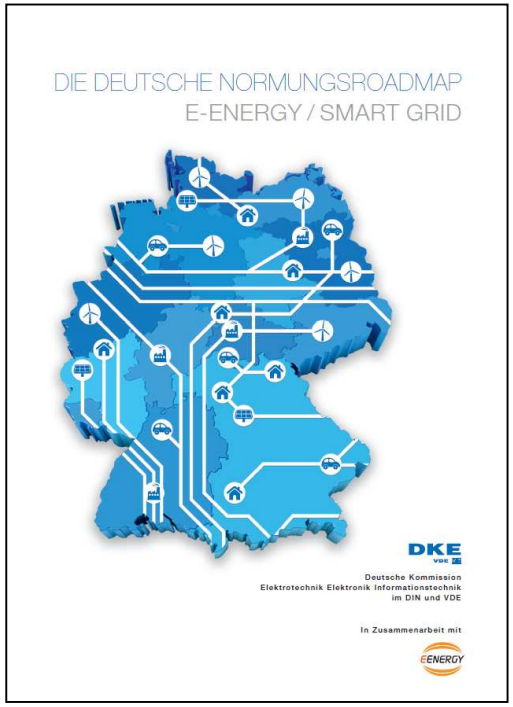
1. E-Energy – Modellebenen



Quelle: EE-Begleitforschung

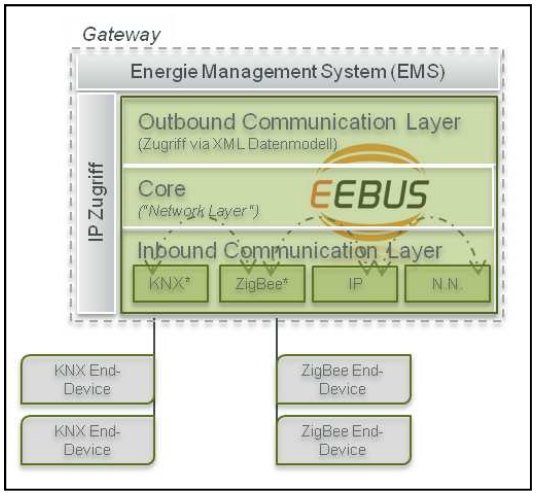
1. E-Energy – Ergebnisse (Beispiele)





EEBus e.V. Initiative

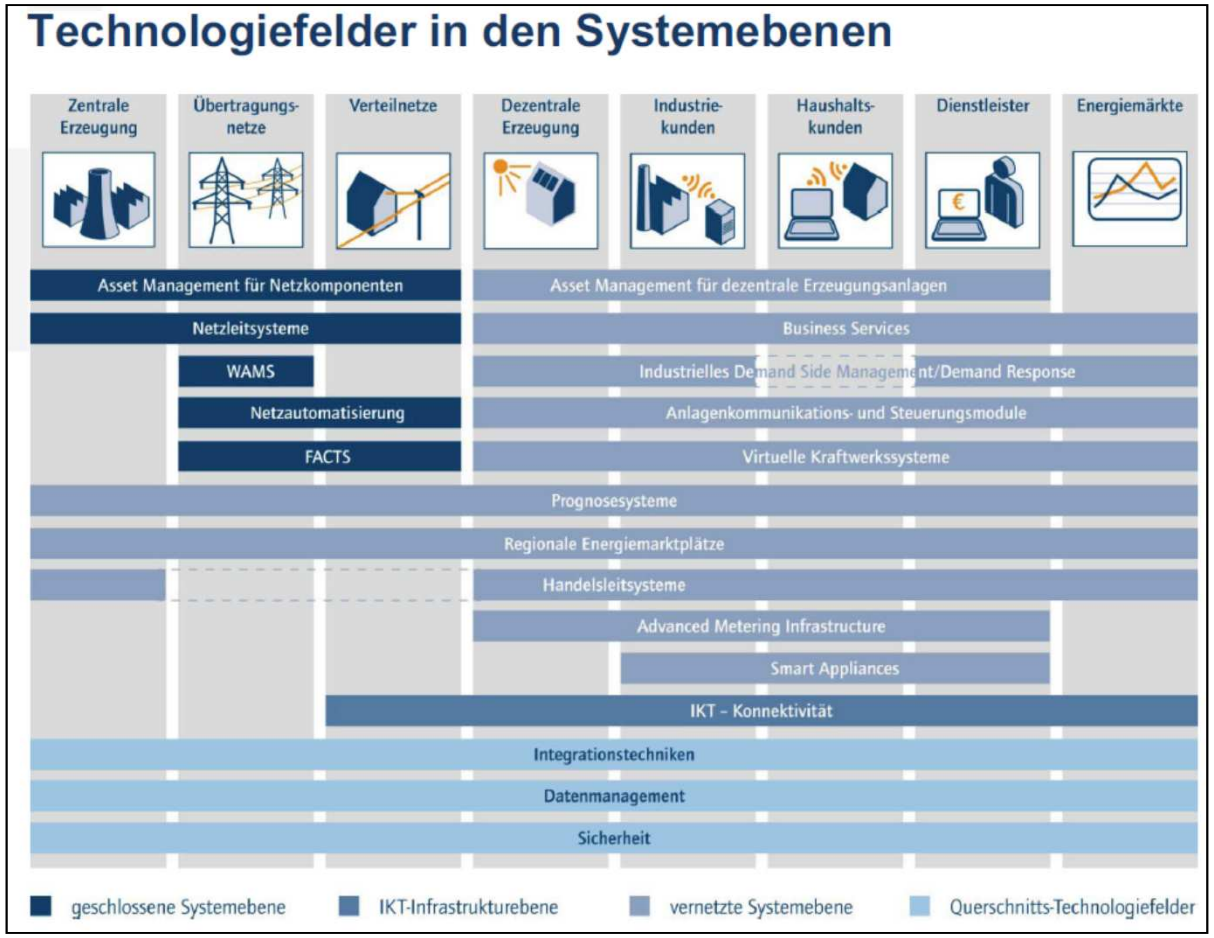
Kommunikationsstandards für Anwendungen und Dienste zur Erhöhung von Komfort und Effizienz im Smart Home



Kontakt: www.e-energy.de

1. E-Energy: Future Energy Grid (FEG)

„Migrationspfade in ein Internet der Energie“



Quelle: acatech

1. E-Energy: Future Energy Grid (FEG)

Technologiefeld 19 – Sicherheit

Fünf Entwicklungsschritte:

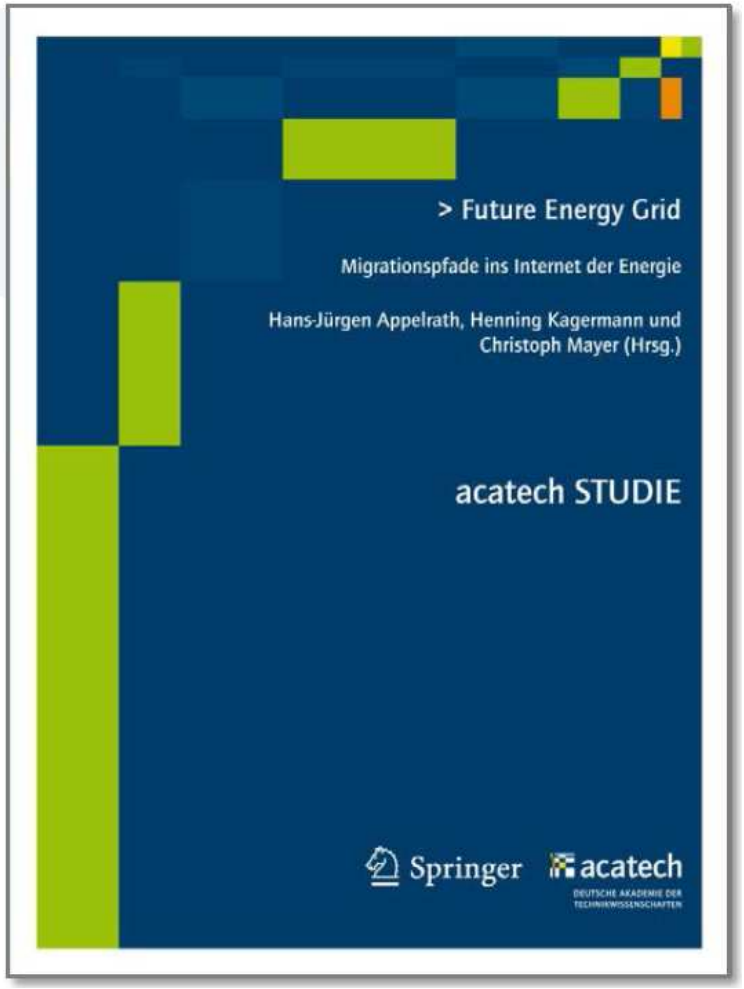
Heute: Sicherheitsanforderungen der Domäne sind bekannt. Allgemeine Sicherheitsstandards sind vorhanden, domänenspezifische Sicherheitsstandards und verbindliche Schutzprofile befinden sich in der Entwicklung. In Smart Grid-Pilotprojekten werden neue Funktionalität erprobt, jedoch der Fokus weniger auf Sicherheit gelegt.

Schritt 1: Vernetzung und Komplexität von Systemen der Energiedomäne nimmt zu. Erhöhte Fehleranfälligkeit und potentielle Angriffsfläche für das Gesamtsystem.

…

Schritt 5: Das Smart Grid ist ein intelligentes sich selbstheilendes System, das auf IT-Angriffe und Teilausfällen von Komponenten semiautomatisiert reagieren kann. …

1. E-Energy: Future Energy Grid (FEG)



Download der Studie unter www.acatech.de/feg

Kontakt:

Dr. Christoph Mayer
Christoph.Mayer@offis.de

1. E-Energy: Studie Smart Grid Sicherheit

Kernfragen:

- In welchem Maße muss das Energieinformationsnetz von anderen bestehenden Datennetzen (z.B. Internet) separiert werden bzw. können bestehende Datennetze für ein Energieinformationsnetz Verwendung finden.
- Welche Anforderungen und Maßnahmen werden an (Sicherheits-) Technologien, organisatorische Maßnahmen und Aufklärung/Beratung, Rechtliche Regelungen sowie Normen und Standards gestellt.
- Ist die Übertragbarkeit von Sicherheitskonzepten aus anderen Anwendungsfeldern auf das Anwendungsgebiet Smart Grid/Smart Energy möglich.

Start: September 2012

Workshops zur Eröffnung und dem Abschluss der Studie

Quelle: acatech

2. SecMobil

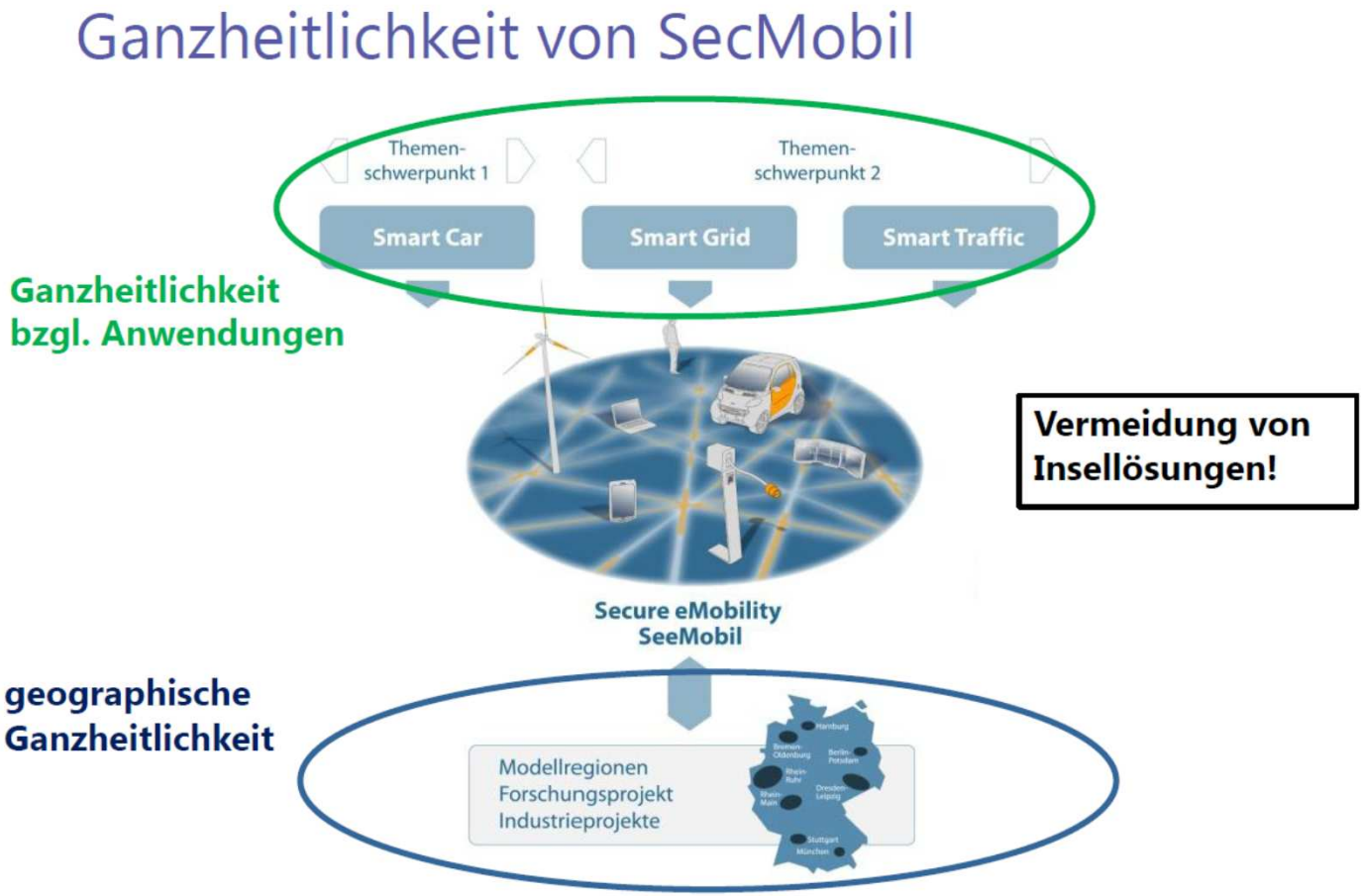
Quelle: escrypt

Querschnittprojekt im Rahmen des Förderprogramms IKT für Elektromobilität II - Smart Car - Smart Grid - Smart Traffic

Ziel: Entwicklung und Erprobung einer standardisierten Sicherheitsarchitektur, die Automobilherstellern, Energieanbietern, Verkehrsbetrieben und Dienste-Anbietern einen vertrauenswürdigen Austausch von Daten erlaubt.

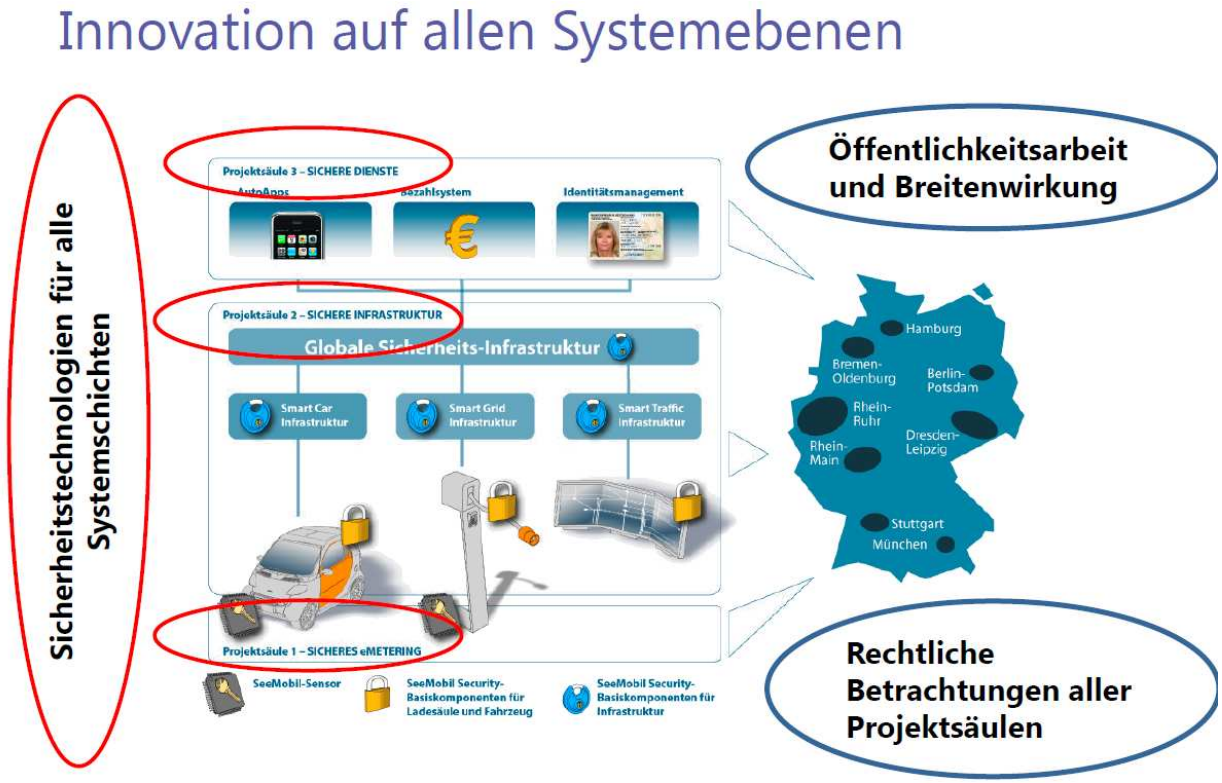
Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

2. SecMobil



Quelle: escrypt

2. SecMobil

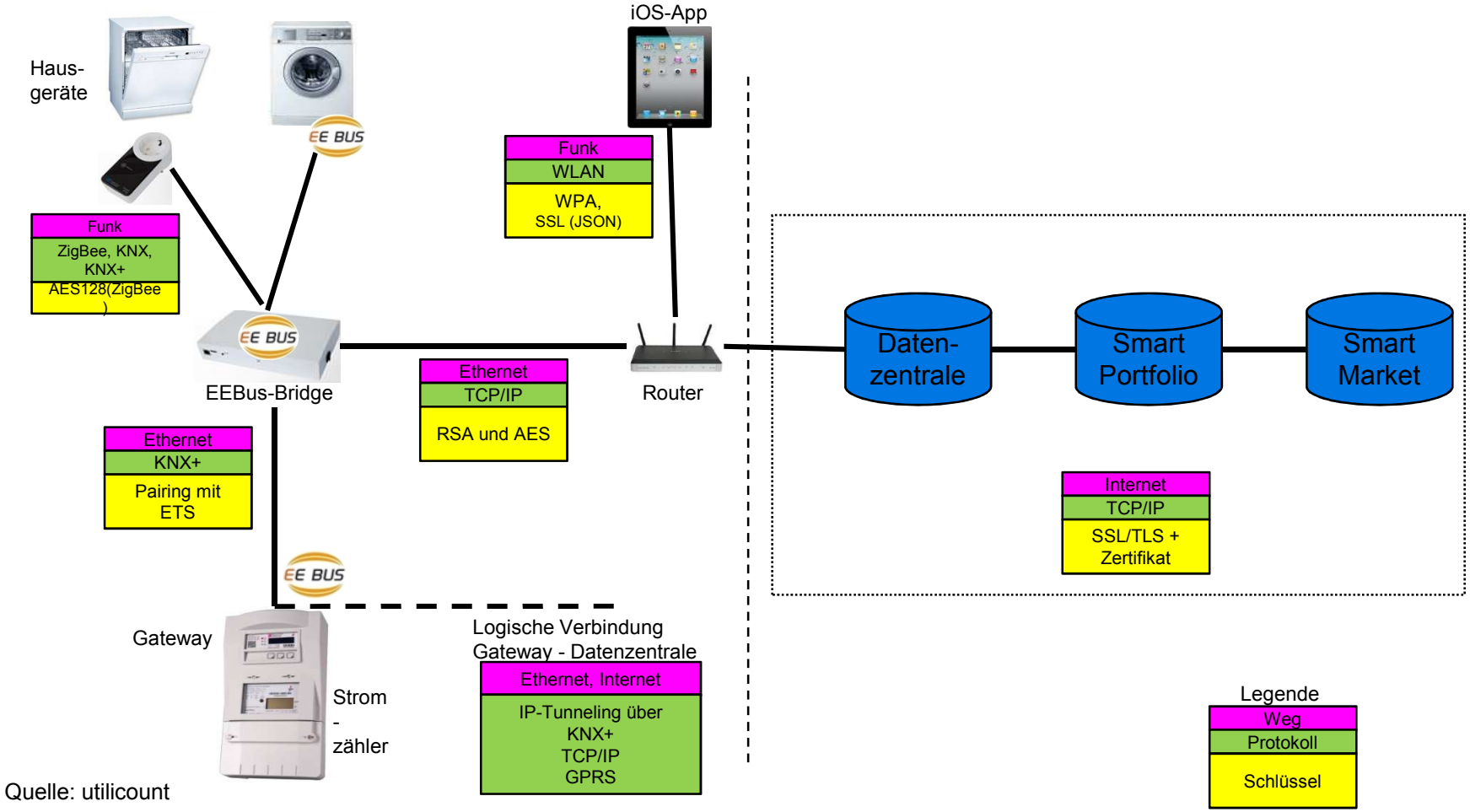


Quelle: escrypt

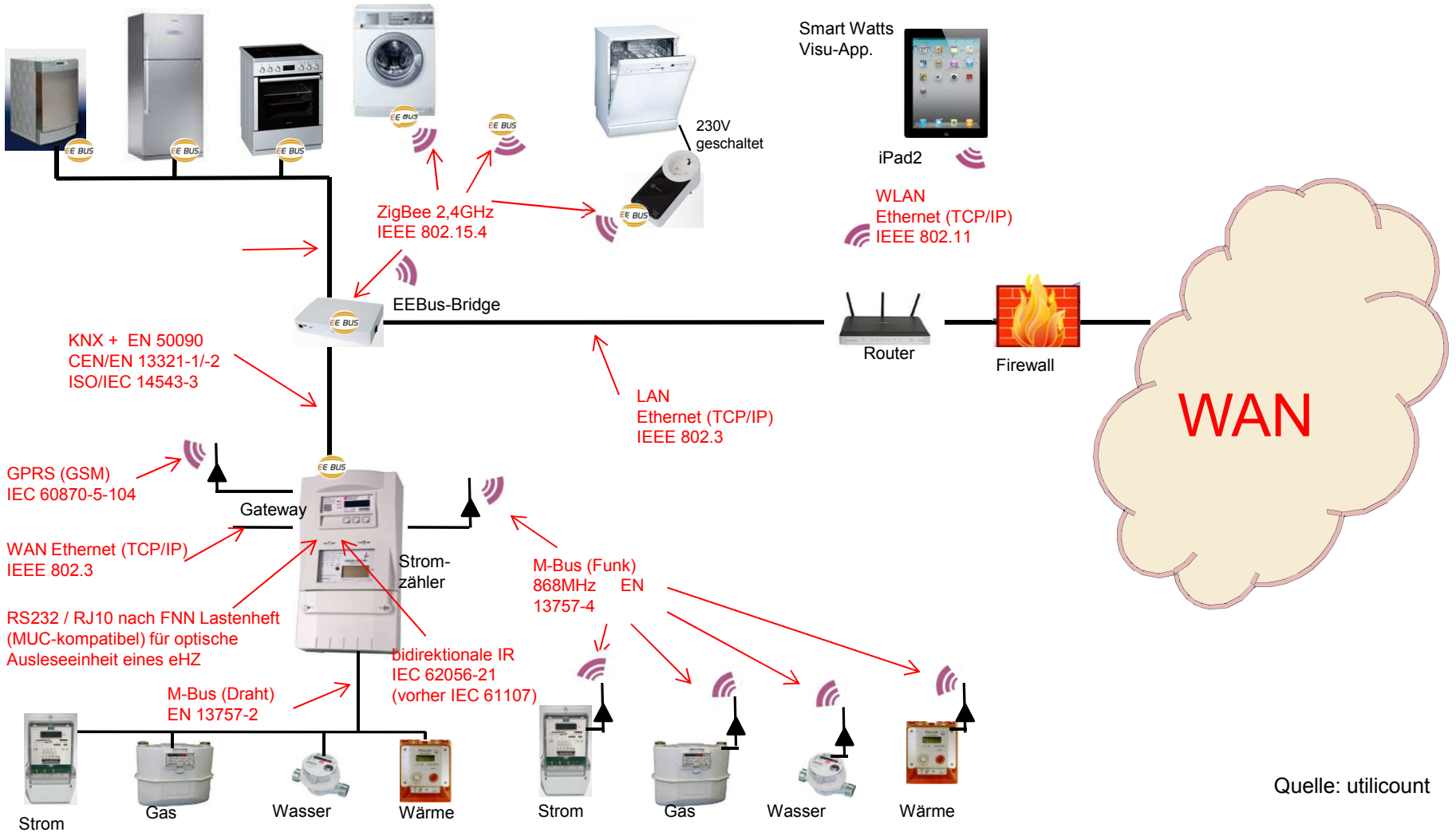
Kontakt: Matthias Küster; ESCRYPT GmbH; matthias.kuester@escrypt.com

3. Smart Watts Sicherheitskonzept

Übersicht Schnittstellen, Protokolle und Verschlüsselung



3. Smart Watts Sicherheitskonzept: Architektur

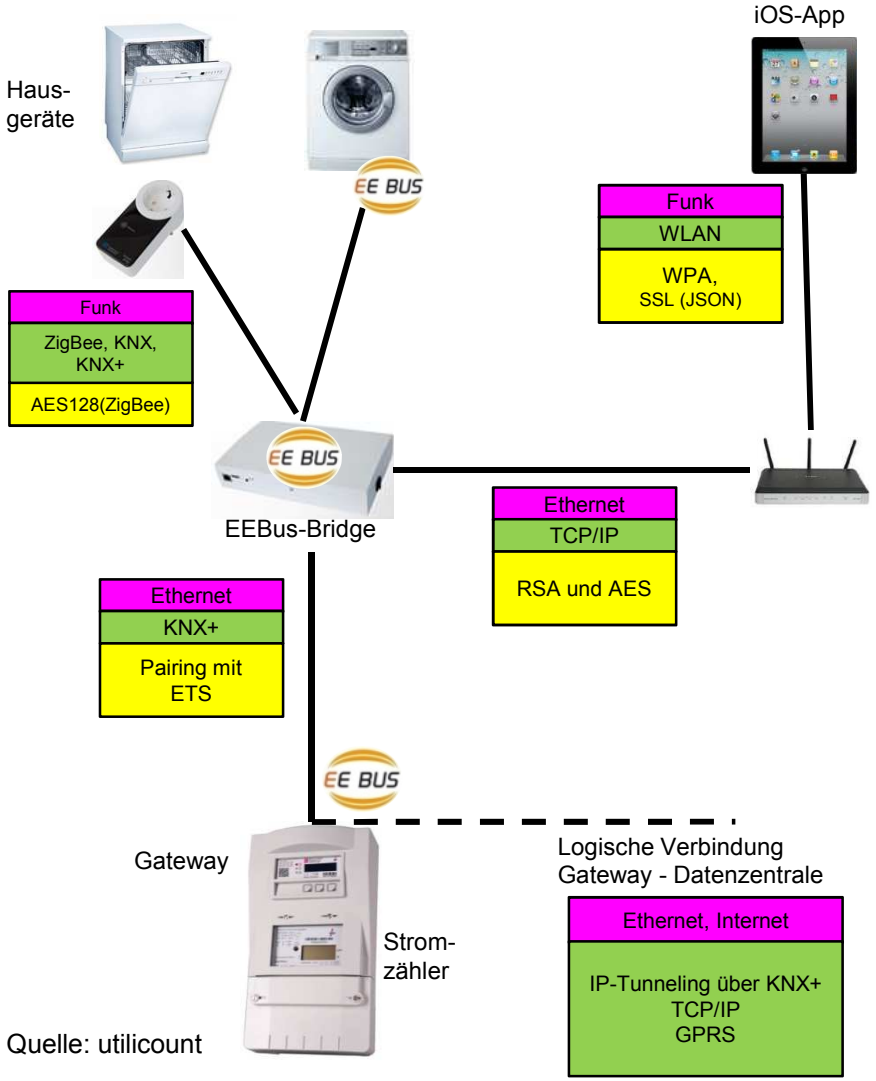


Quelle: utilicount

3. Smart Watts Sicherheitskonzept

Kommunikationsbereich Inhouse

- Bridge und Gateway bilden die Zentrale im Smart Home Netzwerk
- Weitere Komponenten wie Meter, Homedisplay oder Verbrauchsgeräte werden angeschlossen.
- Daten laufen in der Bridge zusammen und werden von dort aus an die verschiedenen Stellen weitergeleitet.
- Je nach Kommunikationsart werden Signale von einem Standard in einen anderen übersetzt.
- Als Übergreifender Standard in der Kommunikation wird der EEBus eingesetzt. Dies bedeutet die Nutzung bestehender Kommunikationsstandards, -normen und Produkte. Innerhalb des EE-Busses sind die Protokolle ZigBee, KNX, KNX+ und IP enthalten um eine umfassende hersteller- und geräteübergreifend Abdeckung zu gewährleisten.



3. Smart Watts Sicherheitskonzept

Stand der Prototypische Feldtestimplementierung:

- Sicherheitsbewertung durch externen Experten im Jan. 2012
- Sicherheitsbetrachtung der Komponenten
    - DSL-Router
    - Server Datenzentrale
    - Server Infoportal
- Analyse der Bedrohungsszenarien
- Festlegung von Sicherheitsmaßnahmen für den sicheren Betrieb einzelner Komponente
- Mehrere Workshops zur spezifischen Sicherheitsbetrachtung
- Modifikationen erfolgt
- Derzeit erfolgt Roll Out für den Friendly User test

Kontakt: Robert Delahaye; utilicount GmbH; r.delahaye@utilicount.com

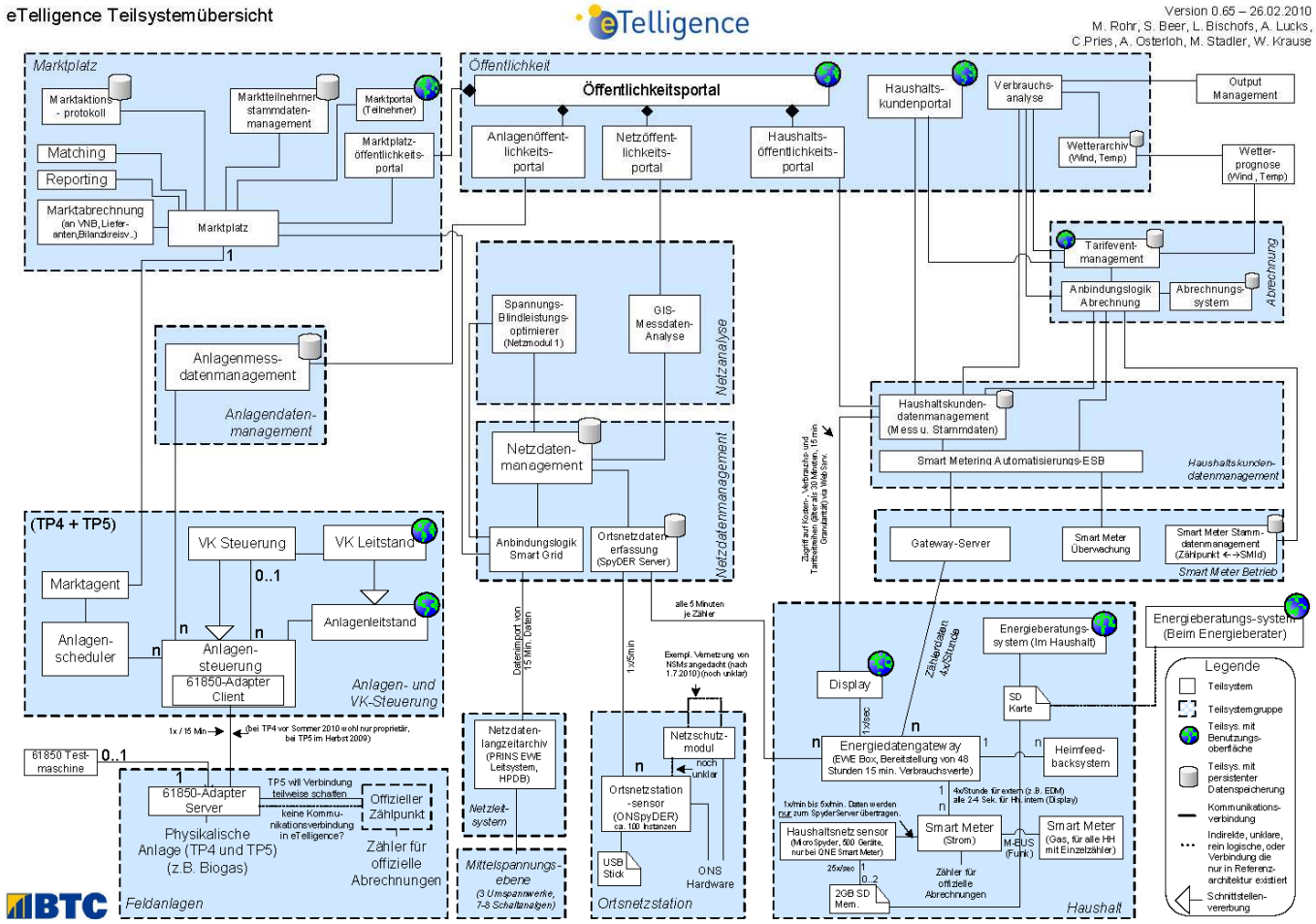
4. Kurzer Überblick zu eTelligence

- E-Energy-Projekt in Modellregion Cuxhaven
- Dauer des Projekts
  - November 2008 bis Oktober 2012
- Kernthema: Verknüpfung von Akteuren der Domäne über IKT auf regionalem Marktplatz für Strom
- TP von OFFIS: Normierung und Sicherheit
  - Betrachtung Informationssicherheitsaspekte

4. Vorgehen bei der Schutzbedarfsanalyse

- Unterteilung der Architektur in Systembereiche
- Bewertung der Schutzziele anhand Bewertungsskala
- Beschreibung beispielhafter Bedrohungsszenarien
- Mögliche Lösungsansätze
- Auswahl von Sicherheitsmaßnahmen

4. eTelligence Teilsystemübersicht



- **Unterteilung in 4 Systembereiche**

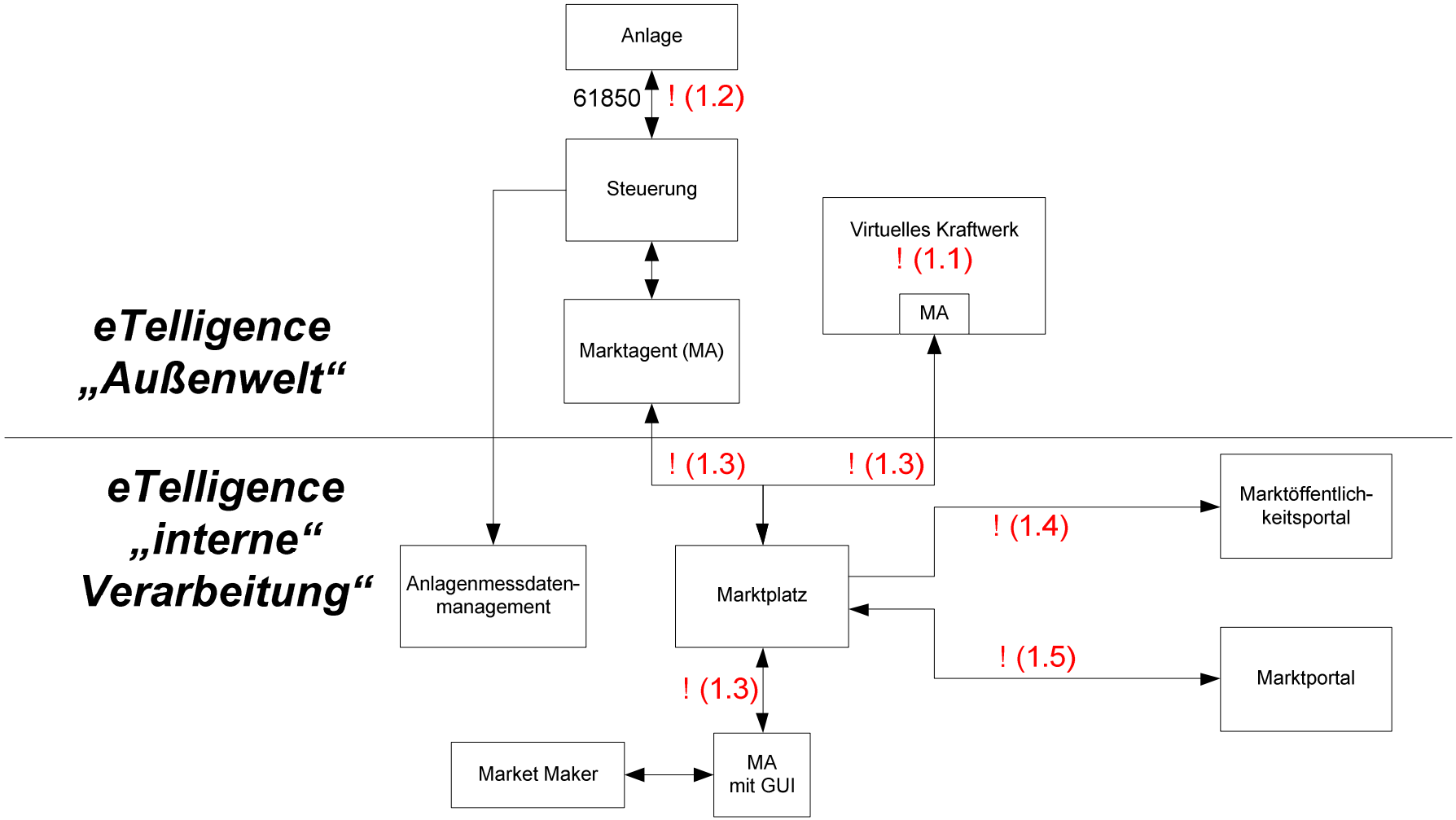
→ **Marktplatz/VK/Anlage**

→ **Öffentlichkeitsportale**

→ **Haushaltsportal/Tarife**

→ **Haushalte/Smart Metering**

4. Beispiel: Sicherheitsrelevante Aspekte im Systembereich Markt/VK/Anlagen



4. Bewertung der Schutzziele

- Einstufung auf Basis des Risikos:
  - 0: Schutzziel muss nicht berücksichtigt werden, hat keine Priorität im Projektkontext.
  - 1: Schutzziel kann erfüllt werden, ist optional (nice-to-have).
  - 2: Schutzziel ist wichtig und sollte nach Möglichkeit erfüllt werden.
  - 3: Schutzziel muss erfüllt werden.

4. Beispiel: Priorisierung Schutzziele für Kommunikation Marktagent und Markt

Schutzziel	Relevanz für konkrete Architektur
Authentizität	3
Integrität	3
Verbindlichkeit	2
Verfügbarkeit	1
Vertraulichkeit	3

4. Beispiel: Sicherheitsmaßnahmen für Kommunikation Marktagent - Marktplattform

- **Authentifizierung mittels Login und Passwort**
  - Absicherung des Schutzziels Authentizität
- **Verwendung eines virtuellen privaten Netzes mit Transportverschlüsselung**
  - Absicherung der Schutzziele Integrität und Vertraulichkeit
- **Einsatz eines Transaktionslogs**
  - Absicherung des Schutzziels Verbindlichkeit
- **Einsatz eines redundanten Systems**
  - Absicherung des Schutzziels Verfügbarkeit

→ Diese Maßnahmen wurden umgesetzt.

4. Weitere Sicherheitsmaßnahmen

- **Systembereich Öffentlichkeitsportale:**

  Hier wurden keine Schutzziele verfolgt. Überprüfung der Sicherheit anhand eines Penetration-Tests durch geschultes Personal der BTC IT-Sicherheit.

- **Systembereich Haushaltskundenportal:**

  Authentizität via Benutzername / Passwort

  Vertraulichkeit via Transportverschlüsselung (https)

- **Systembereich Haushalt / Smart Metering:**

  Übermittlung von Viertelstundenwerten aus dem Haushalt:

  Authentizität via Benutzername / Passwort

  Vertraulichkeit via Transportverschlüsselung (https)

  Übermittlung Sekundenwerte -> iPod: WLAN-Verschlüsselung

4. Bewertung Schutzziele für konkrete eTelligence-Architektur

Nummer sicherheits-relevanter Aspekt	Nummer Schutzziel	Lösungsmaßnahme
1.1	1, 2 und 5	Transportverschlüsselung
	3	Transaktionslog
	4	Anlagen-Notprogramm
1.2	1 bis 5	Absicherung nicht zwangläufig notwendig, da die Systeme innerhalb einer abgeschlossenen Anlage liegen. Wenn Absicherung erfolgen soll, kann dies wie in Aspekt 1.1 umgesetzt werden.
1.3	1	Authentifizierung mittels Nutzername und Passwort
	3	Transaktionslog
	1, 2 und 5	Transportverschlüsselung oder VPN
	4	Bei Bedarf: redundante Auslegung der Server
1.4	1	Authentifizierung mittels Nutzername und Passwort
	2	Falls Absicherung der Integrität notwendig, wenn die Daten z.B. nicht in einem Rechenzetrum liegen, kann eine Transportverschlüsselung eingesetzt werden.
	4	Zwischenspeicherung entsprechender Daten im Portal
	5	Kapselung der Daten durch Webservice
1.5	1, 2, 3, 4 und 5	Absicherung nicht zwangläufig notwendig, da Systeme in gleichem Rechen-zentrum liegen. Wenn Absicherung erfolgen soll, kann dies wie in Aspekt 1.3 umgesetzt werden.
1.6	1	Authentifizierung mittels Nutzername und Passwort
	1, 2 und 5	Einsatz des Multiconnectnetzes
	4	Zwischenspeicherung entsprechender Daten in der (Anlagen-)Steuerung bzw. innerhalb des Monitoringservers

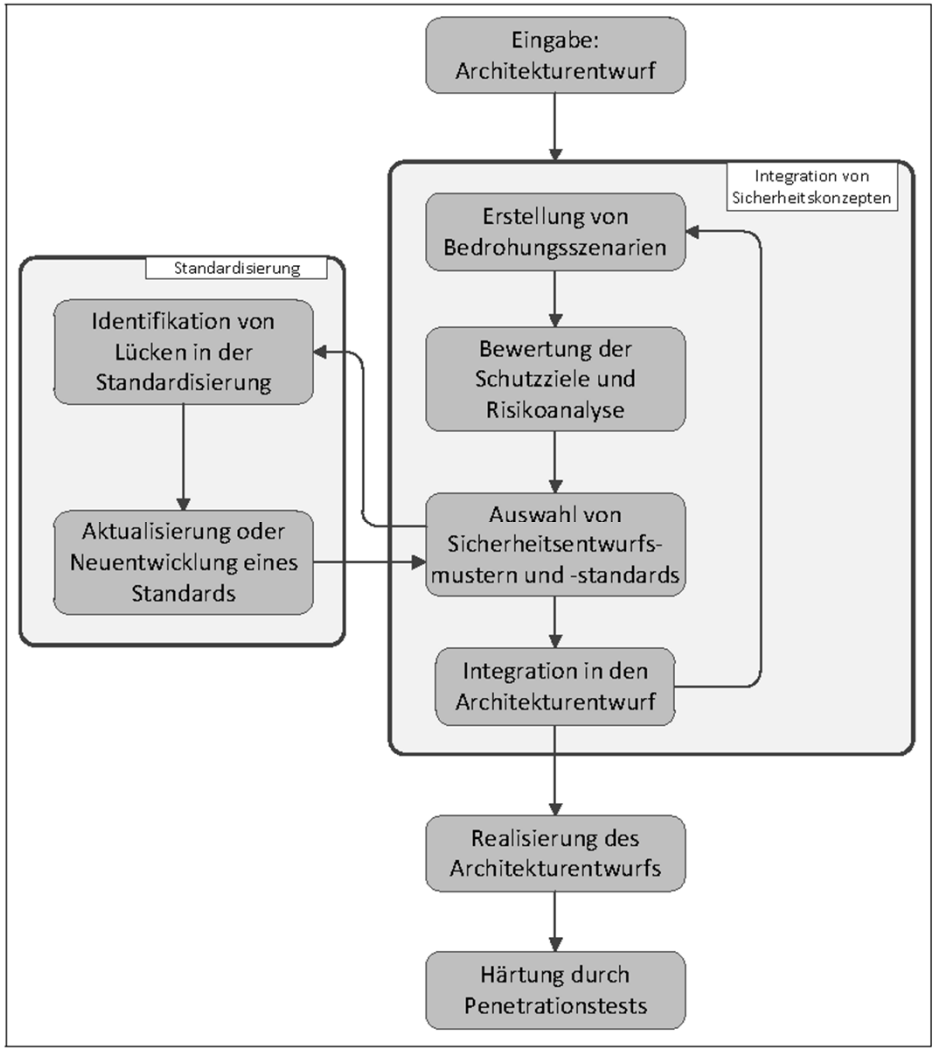
4. Springerbuch: IT-Architekturentwicklung im Smart Grid

ISBN-Nr.: 978-3-642-29207-1

4. Inhalte im Buch

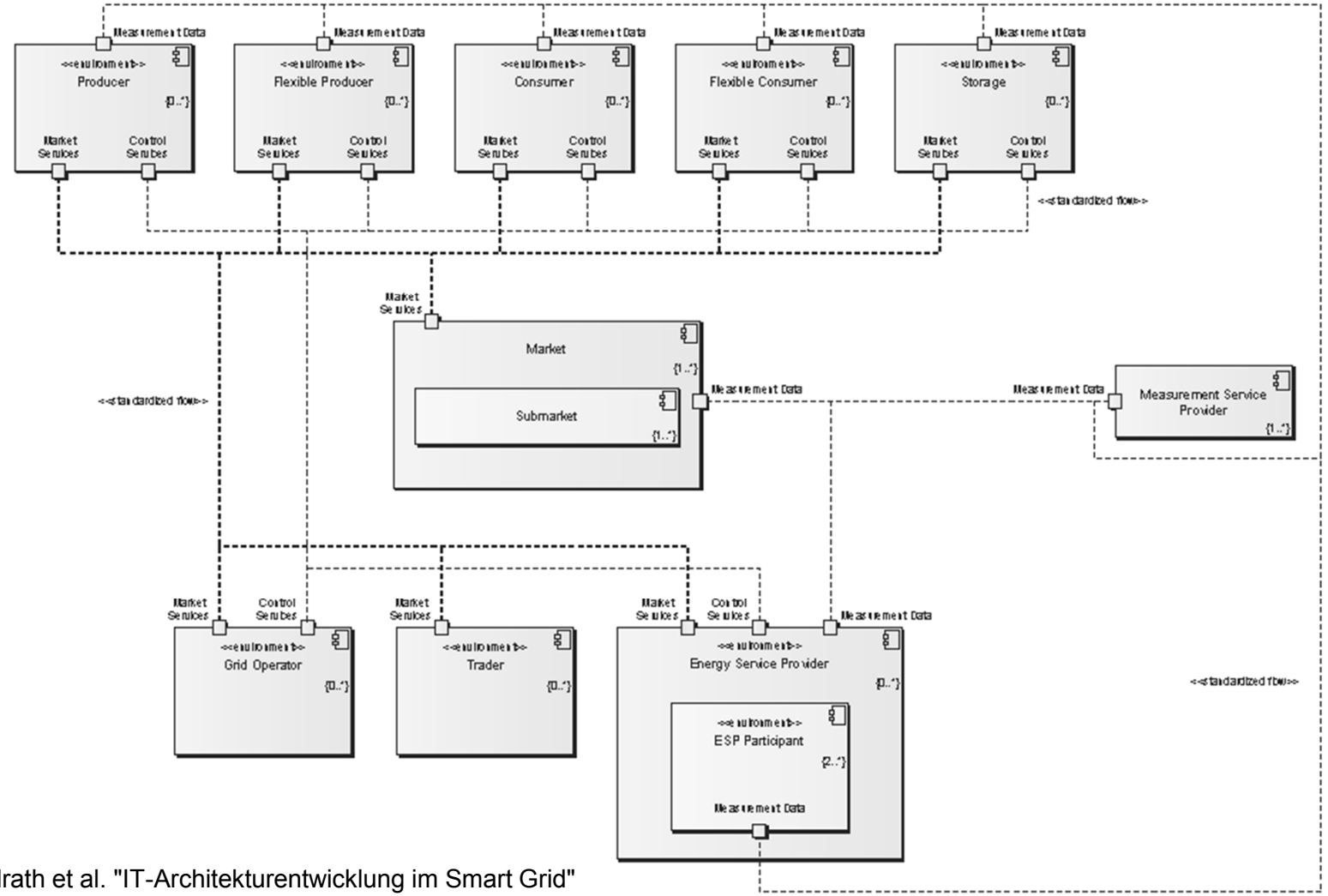
- Beruht auf den Arbeiten von OFFIS in eTelligence
- Unterstützung durch Konsortialpartner BTC und EWE
- Unterteilung der Inhalte in
  - IT-Architekturentwicklung auf Basis von Referenzarchitekturen
    - Informationssicherheit im Smart Grid
  - Umsetzung von IT-Architekturen im Smart Grid
    - Informationssichere Architekturrealisierung

4. Vorgehensmodell: Erstellung Sicherheits-konzept für Referenzarchitektur im Smart Grid



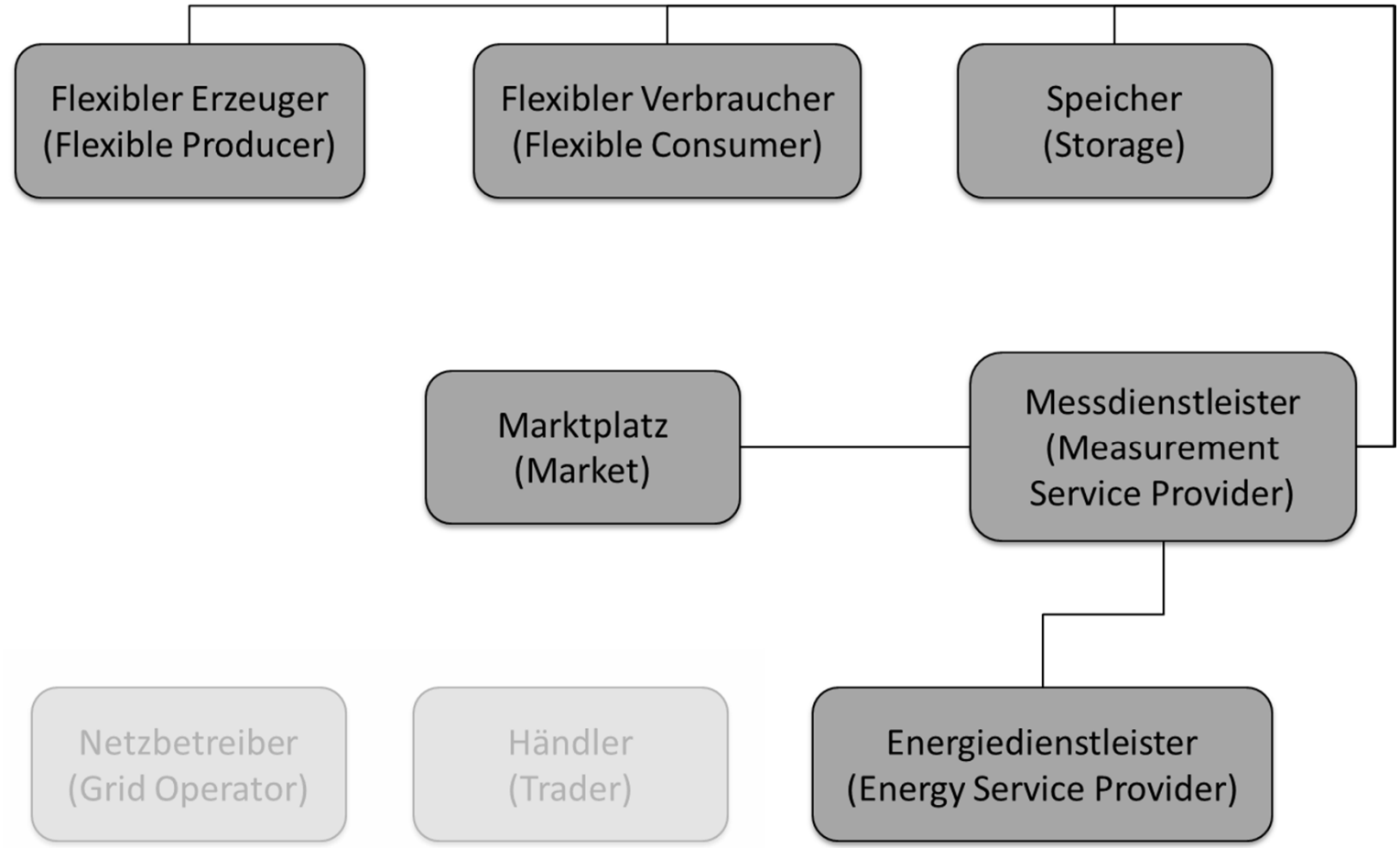
Quelle: Appelrath et al.
"IT-Architekturentwicklung im Smart Grid"

4. eTelligence-Referenzarchitektur



Quelle: Appelrath et al. "IT-Architekturentwicklung im Smart Grid"

4. Beispiel: Messdatenübertragung



Quelle: Appelrath et al. "IT-Architekturentwicklung im Smart Grid"

4. Beispiel: Messdatenübertragung am Beispiel Authentizität

- **Erstellung von Bedrohungsszenarien:**
  - Angreifer manipuliert Authentizität eines Smart Meters
  - Bedrohung: falsche Abrechnung für Erzeuger, Verbraucher oder Speicher
- **Bewertung der Schutzziele und Risikoanalyse:**
  - Schutzbedarfskategorie 3 („hoch“, Schadensauswirkung: beträchtlich)
  - Hohe Schutzbedarfskategorie, für die Absicherung muss Schutzziel intensiv betrachtet werden
- **Auswahl Sicherheitsentwurfsmuster und -standards:**
  - Smart Meter Schutzprofil des BSI
  - AMI-SEC System Security Requirements
  - Passwortbasierte Zugriffskontrolle: Pattern „Password Design and Use“
  - Verwendung von digitalen Signaturen oder auch die Verwendung von Zertifikaten mit oder ohne eigenen Zertifikatsserver über eine PKI
- **Integration in den Architekturentwurf**

4. Sicherheitsstandards für die Domäne Energie

Sicherheitsstandards	SG spezifisch?	Wertschöpfungsbereiche								Titel/Inhalt
		Gewinnung	Energiehandel	Vertrieb	Übertragung	Speicherung	Verteilung	Messung	Anwendung	
IEC 62351- 1-3, 7-10	ja	•	•	•	•	•	•	•	•	Informationssicherheit für Netzführungssysteme und ihren Informationsaustausch
IEC 62351-4, 5	ja	•			•	•	•			Informationssicherheit für Profile einschließlich MMS, sowie für IEC 60870-5 und dessen Derivate
IEC 62443/ISA 99	ja	•	•	•	•	•	•	•	•	Vorgehensmodell zur Herstellung von IT-Sicherheit für die industrielle Automatisierung und Kontrollsysteme
VDI/VDE 2182	ja	•	•	•	•	•	•	•	•	Informationssicherheit in der industriellen Automatisierung
NAMUR NA 115	ja	•	•	•	•	•	•	•	•	IT-Sicherheit für Systeme der Automatisierungstechnik
ISO 27XXX	nein	•	•	•	•	•	•	•	•	Internationale allgemeine Standards für Informationssicherheit

Quelle: Appelrath et al. "IT-Architekturentwicklung im Smart Grid"

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:

Günter Seher
Programmleiter E-Energy
Projektträger Multimedia im DLR
Tel: +49 2203 601-3038
E-Mail: guenter.seher@dlr.de

Christine Rosinger
OFFIS
FuE Bereich Energie | R&D Division Energy
Tel: +49 441 9722 – 175
E-Mail: christine.rosinger@offis.de