
Sicherheitsdomänen im Energieinformationsnetz

Claudia Eckert

Fraunhofer AISEC und TU München

Fachkonferenz Bürgernahe Sicherheitskommunikation für Städte & Gemeinden

13.6. 2012, Berlin



Überblick

1. Motivation

IKT als Nervensystem des SmartGrid

2. Domänen-orientierter Ansatz

Teile und Herrsche: Komplexitätsreduktion

3. Beispiel Domäne Privatkunde

4. Beispiel Domäne Verteilnetz

5. Take Home Message

Überblick

1. Motivation

IKT als Nervensystem des SmartGrid

2. Domänen-orientierter Ansatz

Teile und Herrsche: Komplexitätsreduktion

3. Domäne Privatkunde

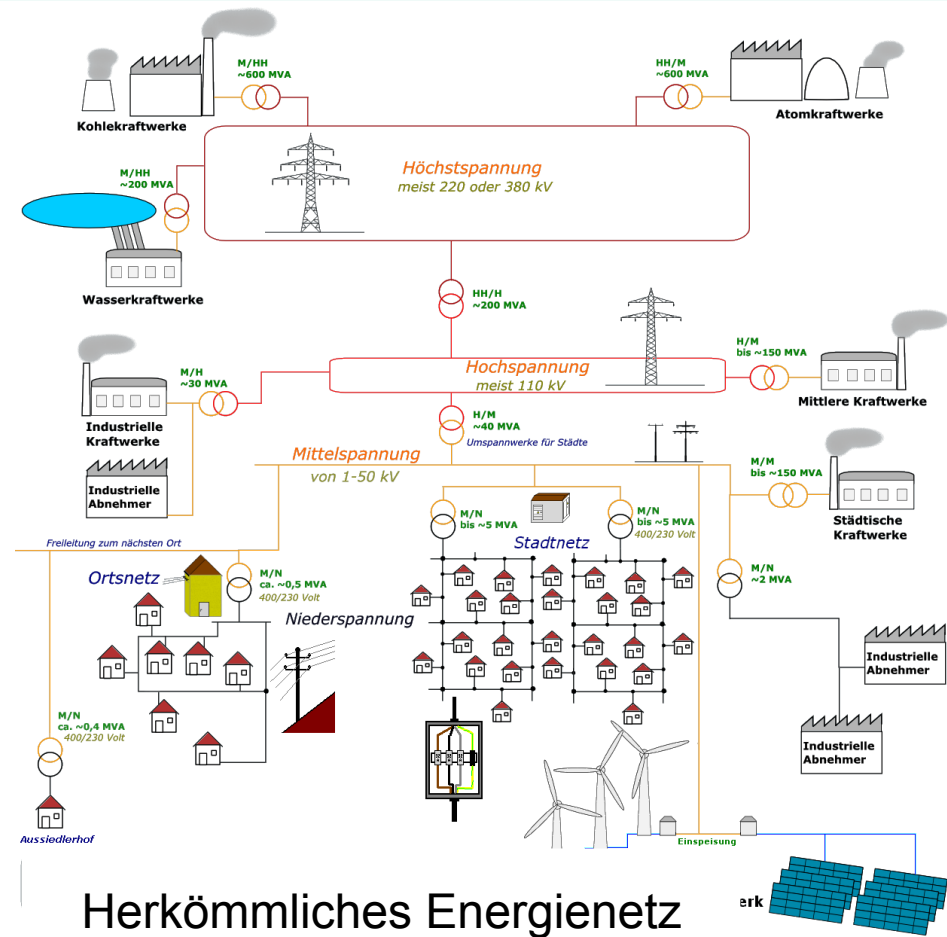
4. Domäne Verteilnetz

5. Take Home Message

1. Motivation

Energienetz

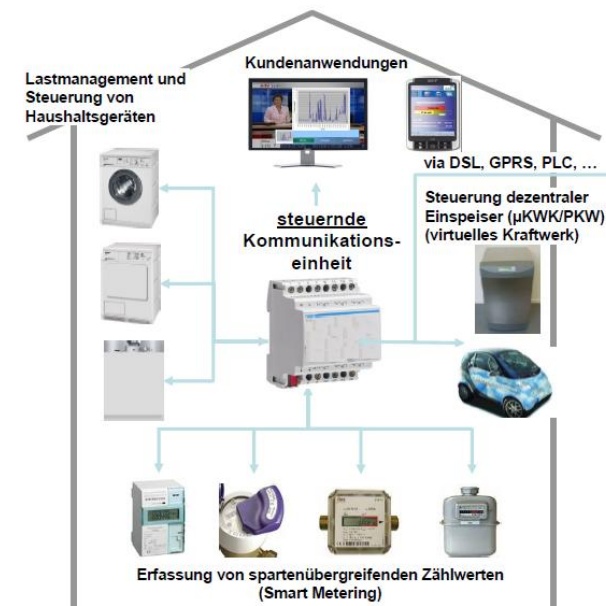
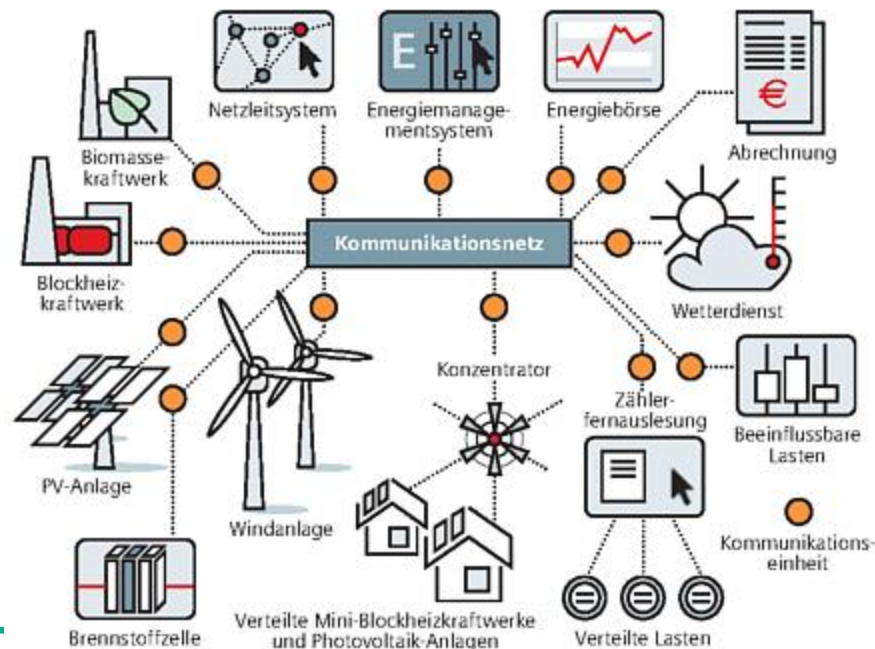
- Dezentrale Energie-
Erzeugung
- Erneuerbare Energie
hohe Schwankungen
- Energie-Transport,
-Speicherung
- Energiemarktplätze



1. Motivation

IKT ist das „Nervensystem“ des SmartGrid

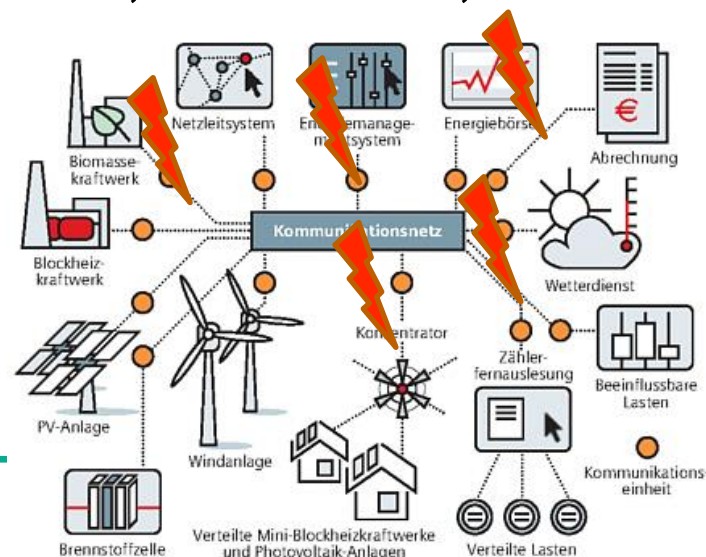
- **Steuerung und Überwachung** der Versorgungssicherheit
- **Daten** zur Steuerung essentiell: **korrekt, vollständig, rechtzeitig**



1.Motivation

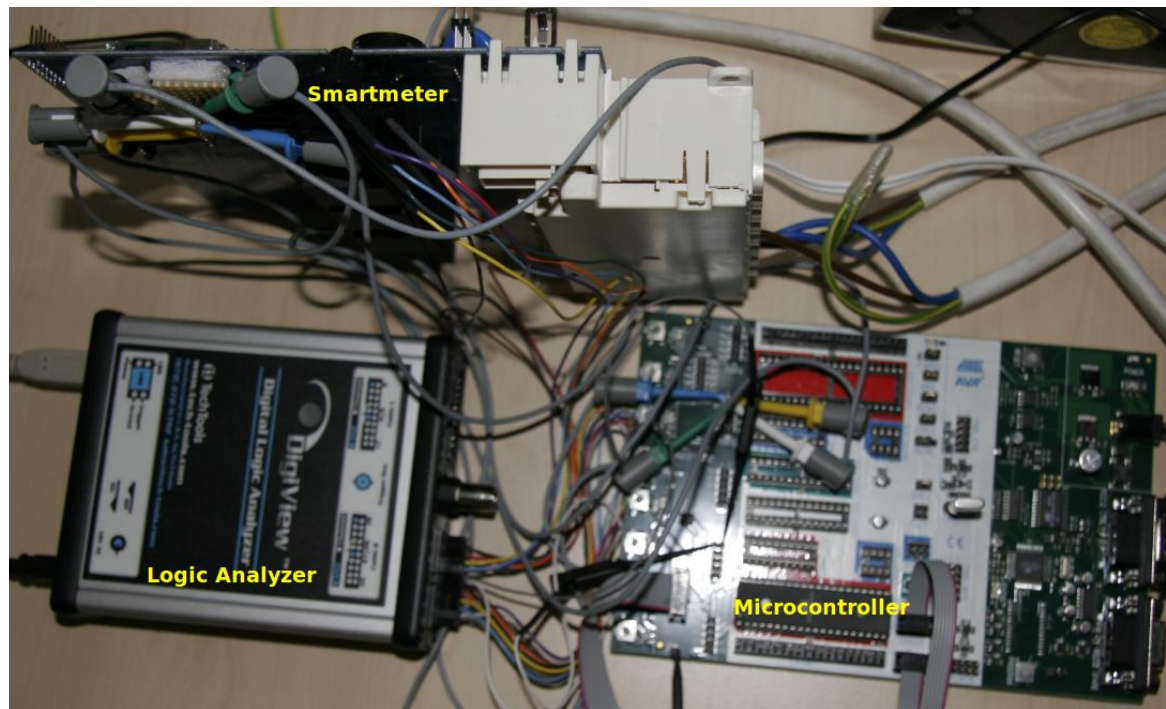
Verwundbarkeit des ‚Nervensystems‘:

- Gezielte Störung der **Betriebssicherheit** durch Angriffe: Manipulierte, veraltete, unvollständige Daten
- Gezielte Störung von (**Geschäfts-)Prozessen** durch Angriffe: gefälschte Identität, Überfluten, falsche Abrechnung, ...



1.Motivation

Angriffe auf Smart Meter: (Fhl-AISEC)

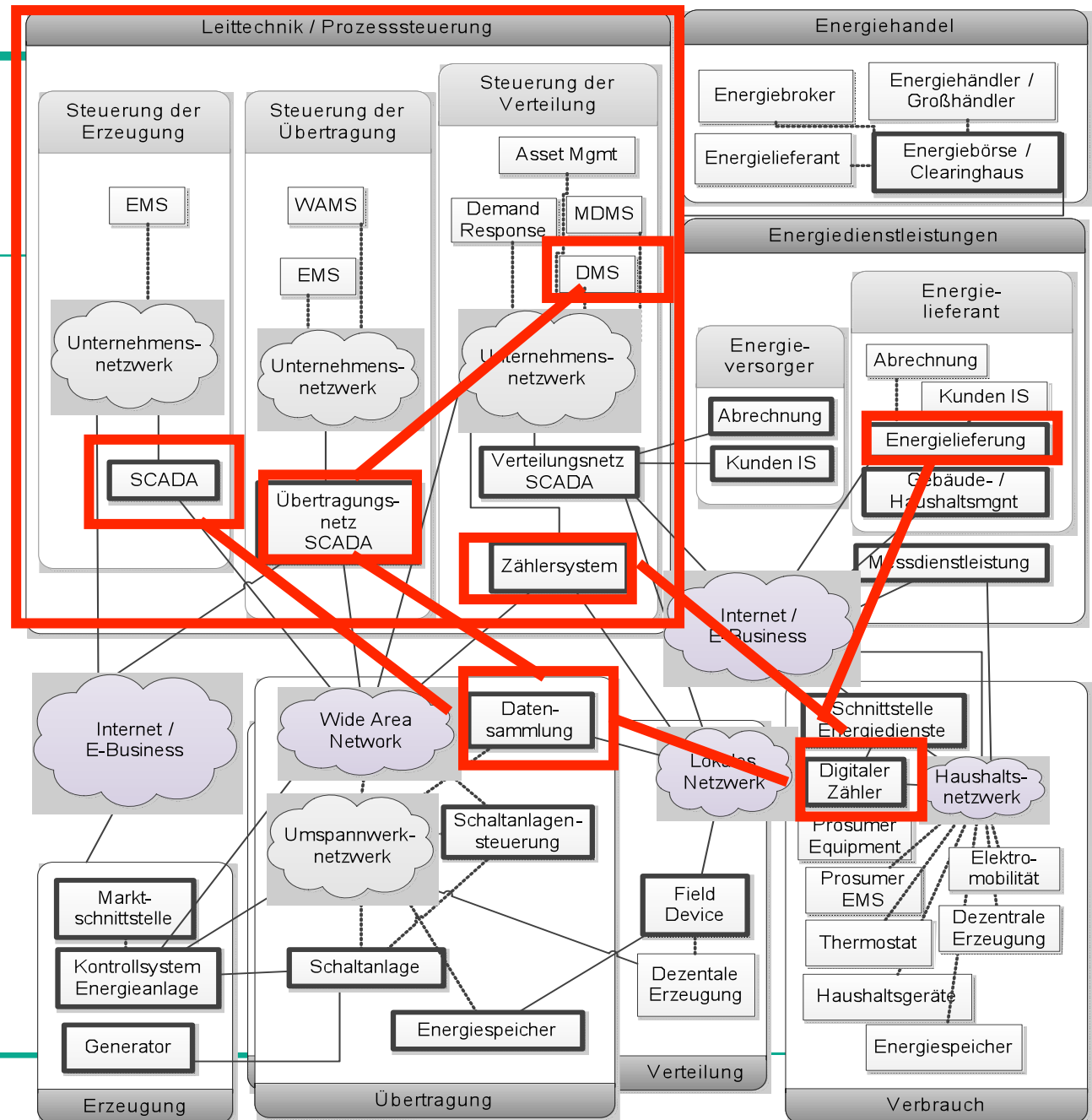


- Daten-Manipulation, Einschleusen von Daten, Abhören, ...

1. Motivation

SmartGrid:

- Tatort &
- Tatwaffe



Herausforderungen

- Sehr **komplexe, heterogene** IKT Infrastruktur
- Viele Marktteilnehmer mit **unterschiedlichen Aufgaben, Rechten, Geschäftsinteressen**
- One-size-fits-all Lösung ist weder **möglich, noch wünschenswert**
- Notwendig: Systematik für **anpassbare, angemessene** Sicherheitslevel

Überblick

1. Motivation

IKT als Nervensystem des SmartGrid

2. Domänen-orientierter Ansatz

Teile und Herrsche: Komplexitätsreduktion

3. Domäne Privatkunde

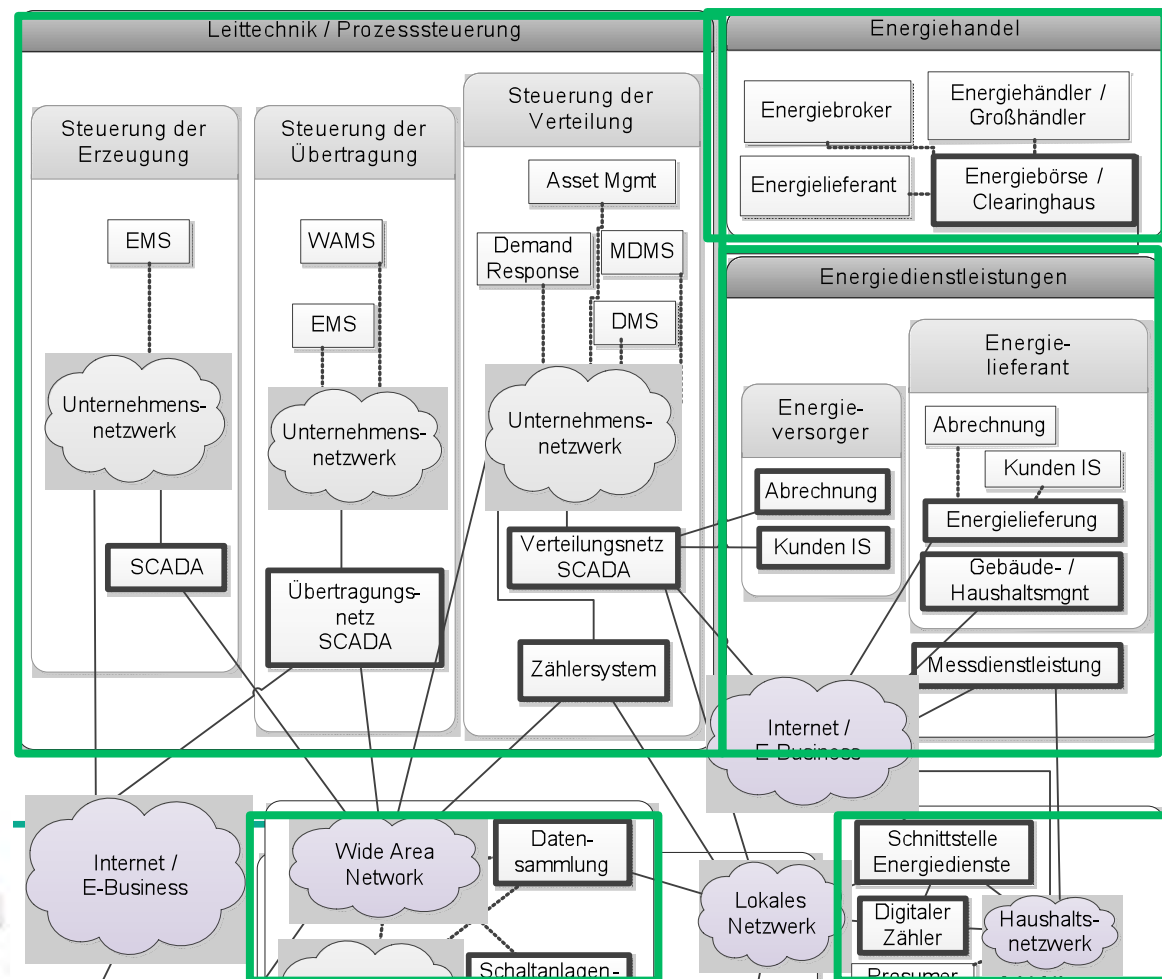
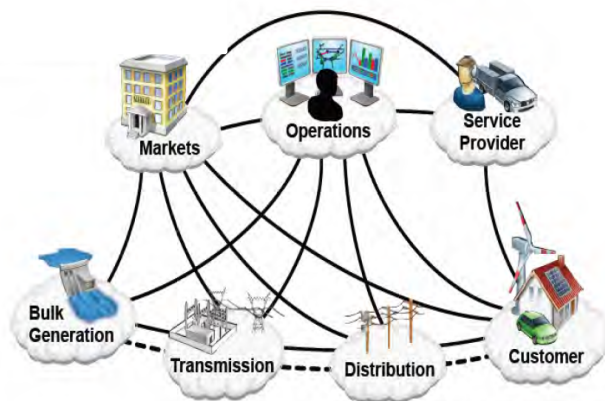
4. Domäne Verteilnetz

5. Take Home Message

2. Domänen-basierter Ansatz

Identifikation von Domänen

- Erzeugung
- Verteilung
- Handel
- Kunde
- ...

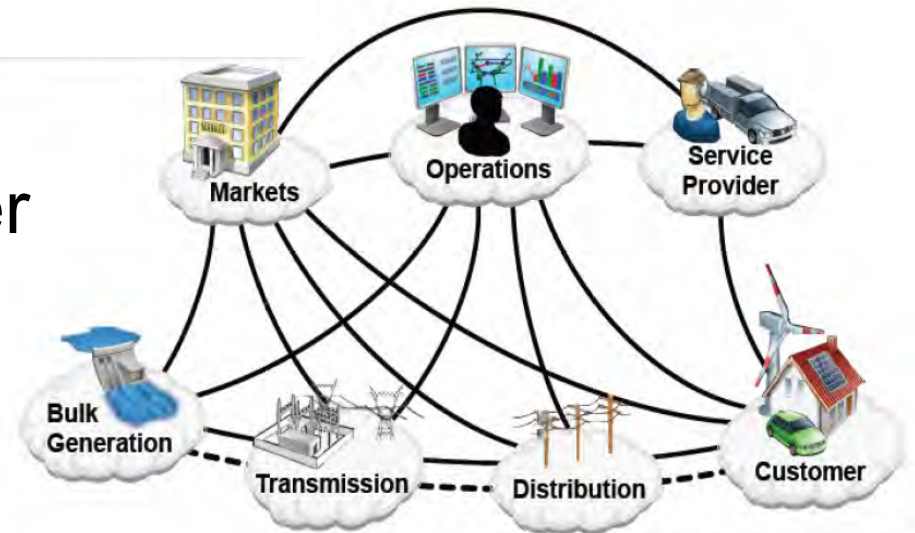


2. Domänen-basierter Ansatz

Für jede Domäne:

Rollen

- z.B. Kunde, Netzbetreiber
- **Use-Cases**
 - z.B. Fernzugriff, messen
- **Abgeleitet Anforderungen**
 - z.B. korrekte Steuerungsdaten
- **Sicherheitsarchitektur:**
 - Rollenspezifische Rechte und Pflichten
- **Angepasste Sicherheitskonzepte:** IDs, Schlüssel



Überblick

1. Motivation

IKT als Nervensystem des SmartGrid

2. Domänen-orientierter Ansatz

Teile und Herrsche: Komplexitätsreduktion

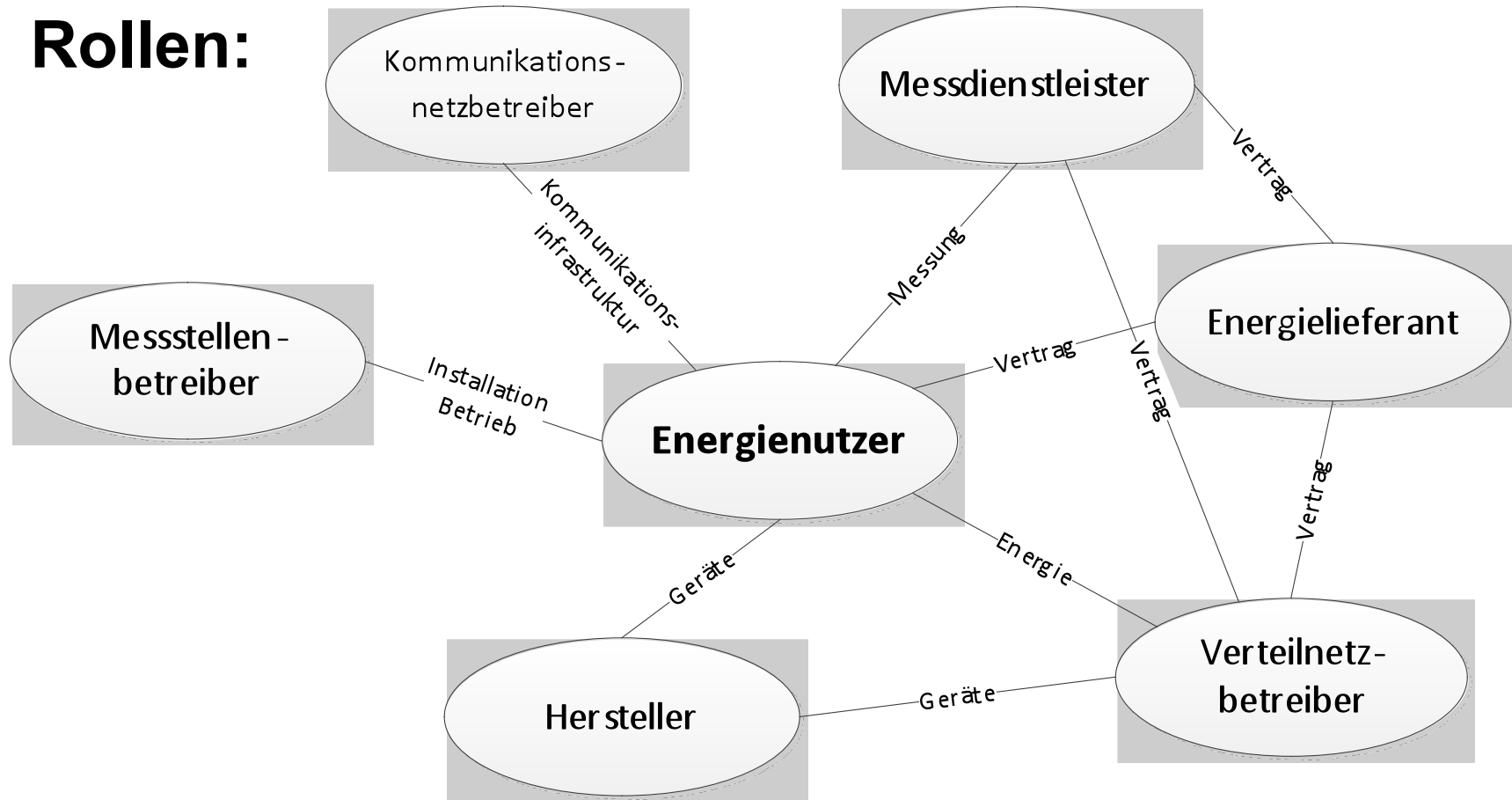
3. Beispiel Domäne Privatkunde

4. Domäne Verteilnetz

5. Take Home Message

3. Domäne Privatkunde

Rollen:



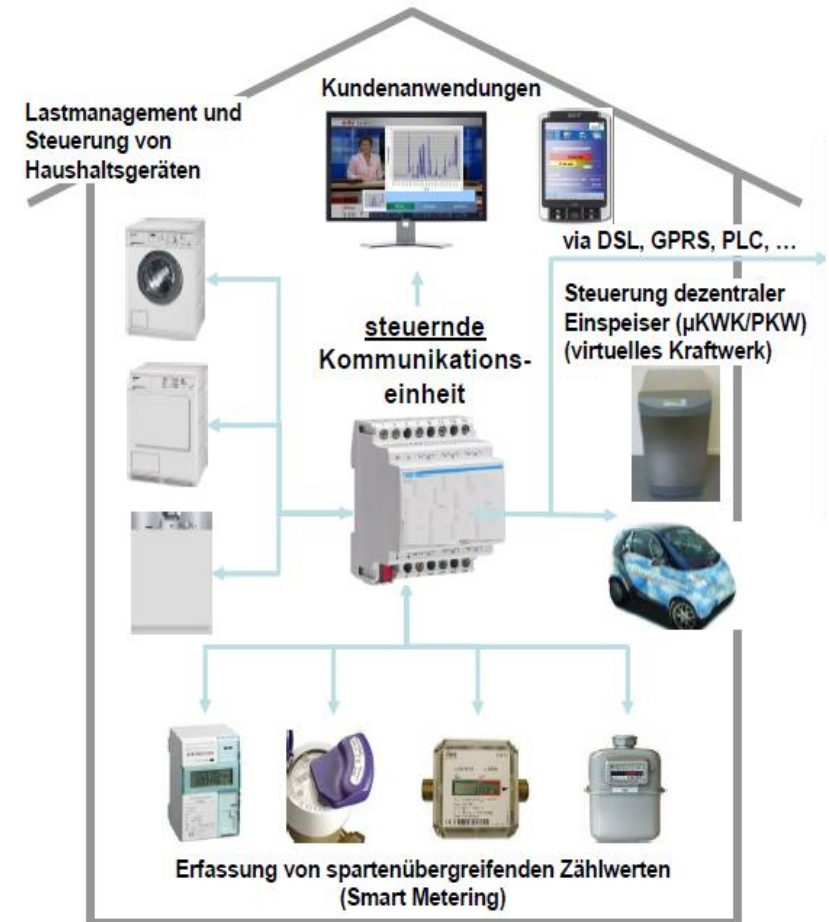
3. Domäne Privatkunde

Use-Cases u.a.

- Messwerterfassung
- (Fern)-Wartung
- Tarifierung (dynamisch)

Sicherheitsanforderungen

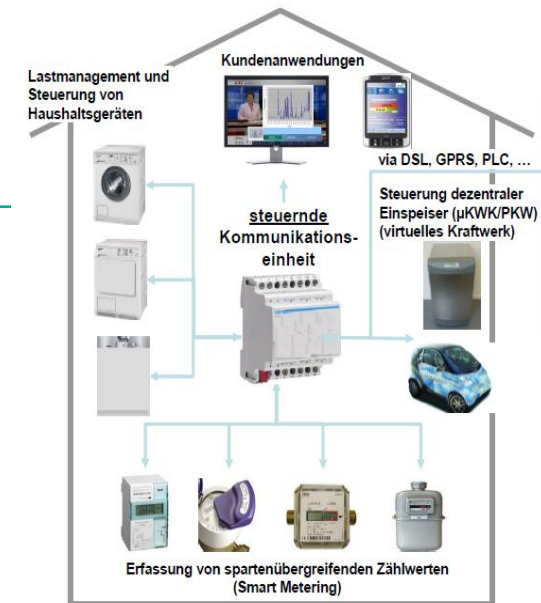
- Rollen-abhängige Pflichten
Abrechnen, Warten, ...
- Use-case abhängige Daten:
Verbrauchsdaten, Steuerungsdaten



3. Domäne Privatkunde

Rolle **Energienutzer**:

- **Relevante Daten:** Verbrauch, Abrechnung
- **Anforderungen**
 - **Vertraulichkeit** von Verbrauchswerten,
 - **Vertraulichkeit** der Abrechnungsdaten
 - **Korrektheit, Zuordenbarkeit** von Messwerten, Abrechnungs-, Wartungsdaten (Patches etc.)
 - **Versorgungssicherheit**

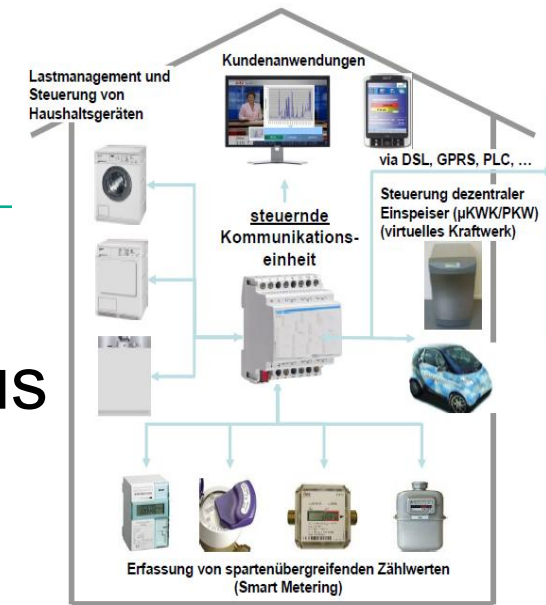


3. Domäne Privatkunde

Rolle **Verteilnetzbetreiber**:

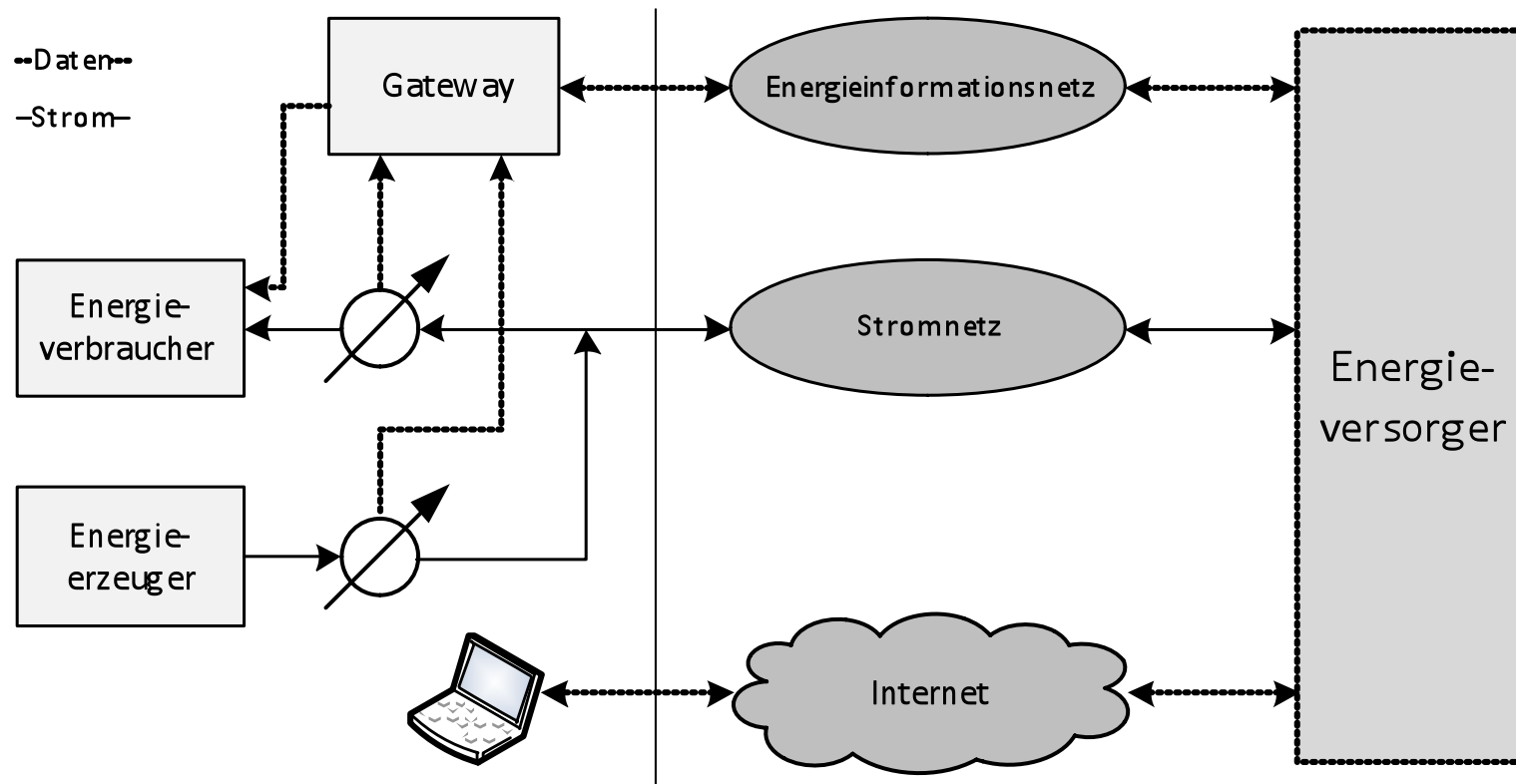
- **Relevante Daten:** Steuerung, Status
- **Anforderungen**
 - **Versorgungssicherheit:**
Prognose, Status
 - **Korrektheit** von **aggregierten** Messwerten
 - **Korrektheit und Aktualität** von Steuerdaten
 - **Korrektheit** von Wartungsdaten

Fazit: Mehrseitige, ggf konträre Anforderungen



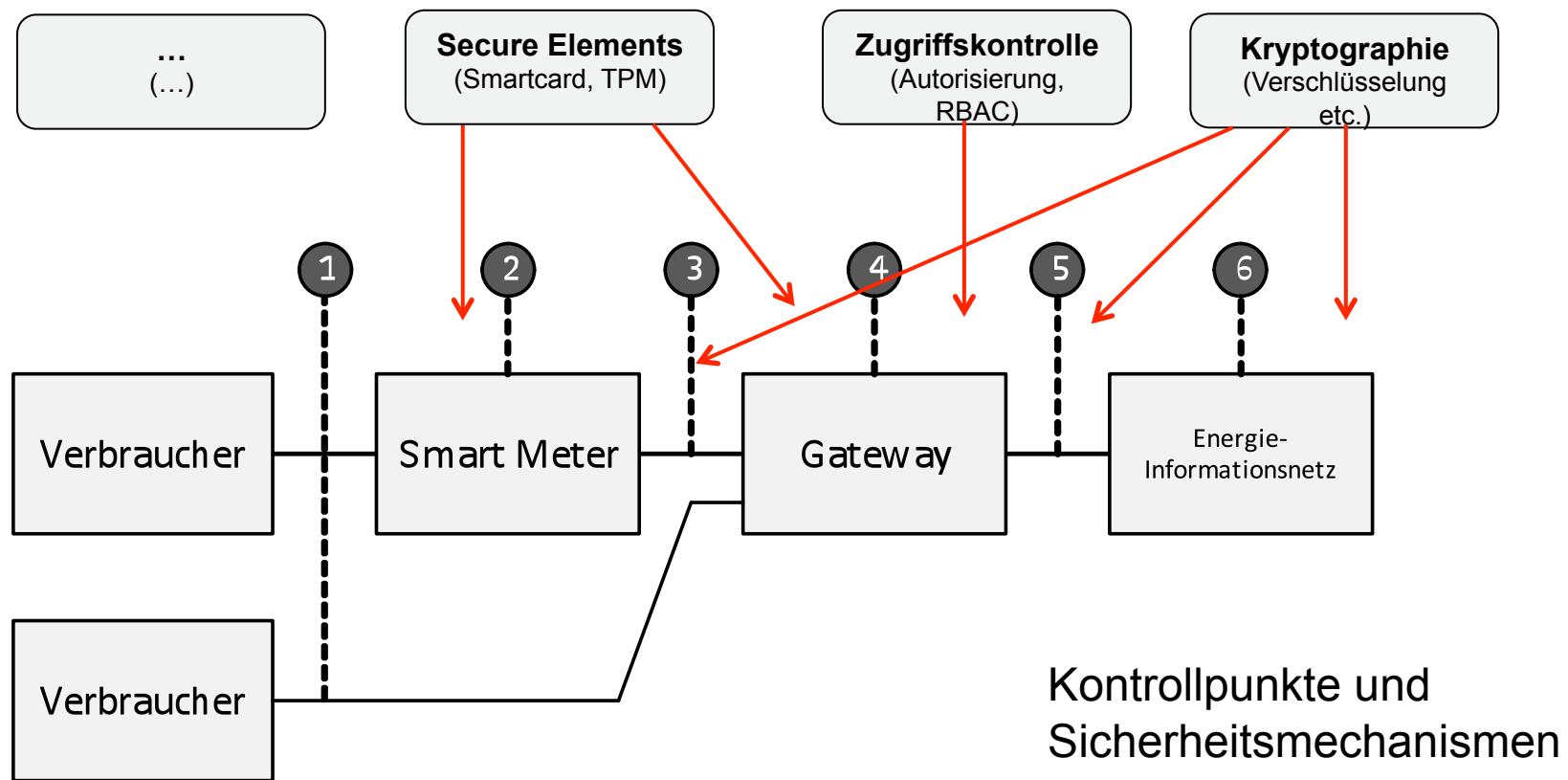
3. Domäne Privatkunde

Referenzarchitektur



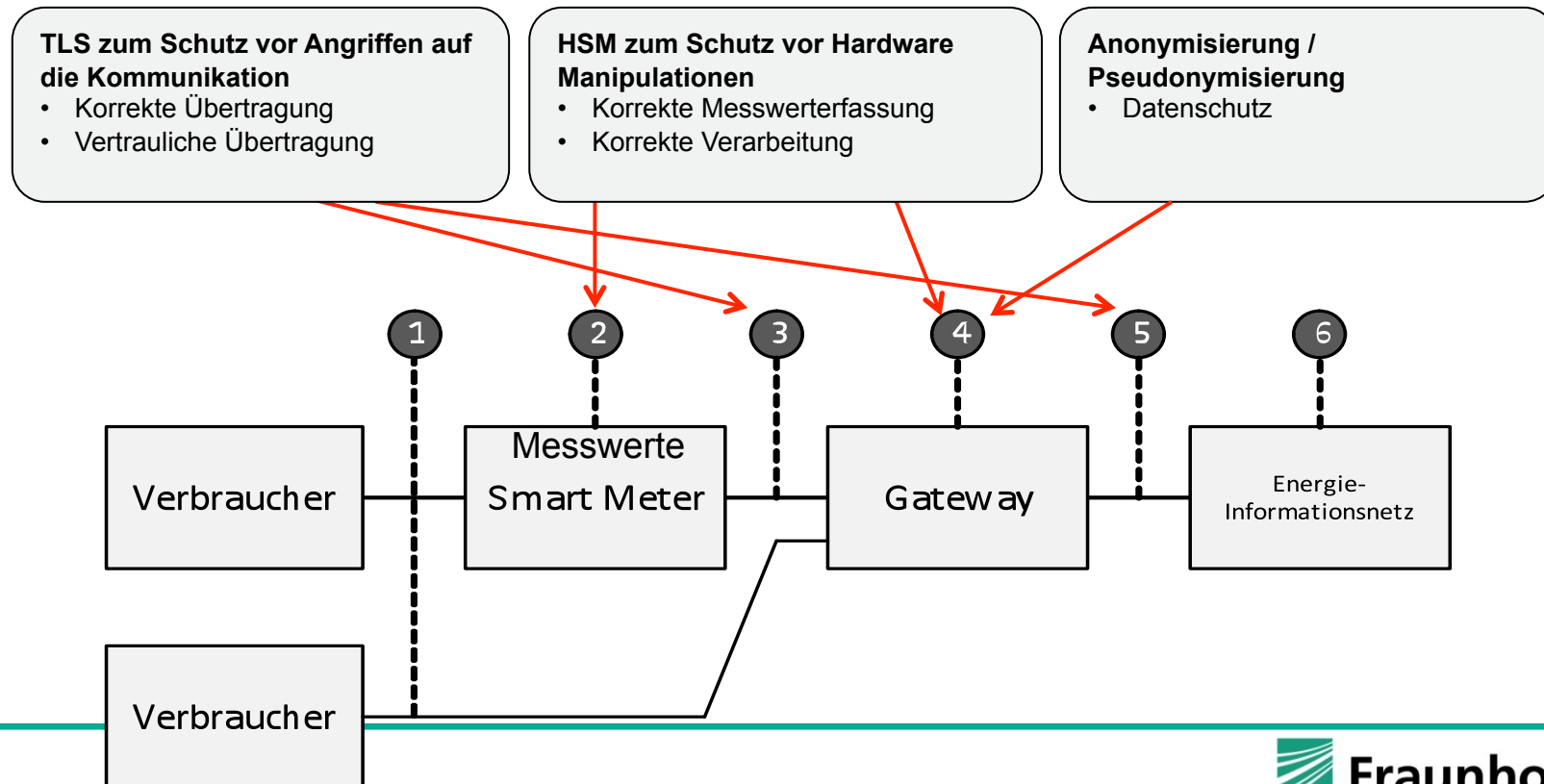
3. Domäne Privatkunde

Sicherheits-Architektur & -Konzepte:



3. Domäne Privatkunde

Konkretisierung: Sichere Messwerterfassung und – übertragung

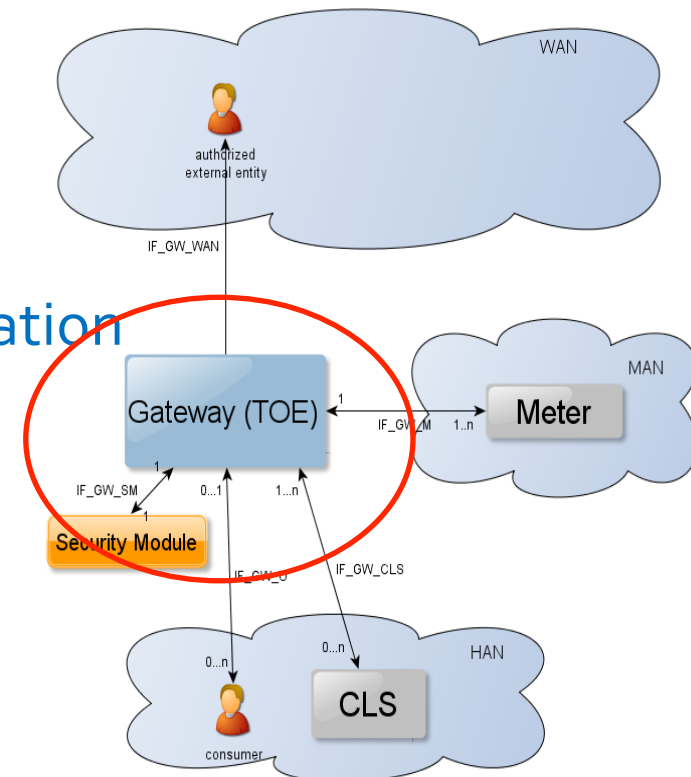
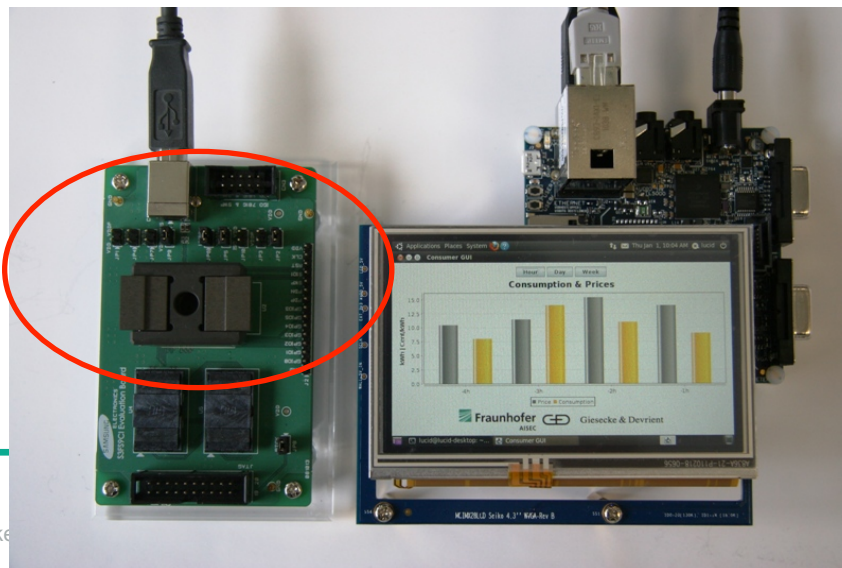


3. Domäne Privatkunde

Sicherer Smart Meter/sicheres Gateway: FhI-AISEC u. G&D

- Basis: [BSI Protection Profile](#)
- Sicherheits-Modul: JavaCard

Authentisierung, Verschlüsselung,
manipulationssicher, Daten-Aggregation



Überblick

1. Motivation

IKT als Nervensystem des SmartGrid

2. Domänen-orientierter Ansatz

Teile und Herrsche: Komplexitätsreduktion

3. Domäne Privatkunde

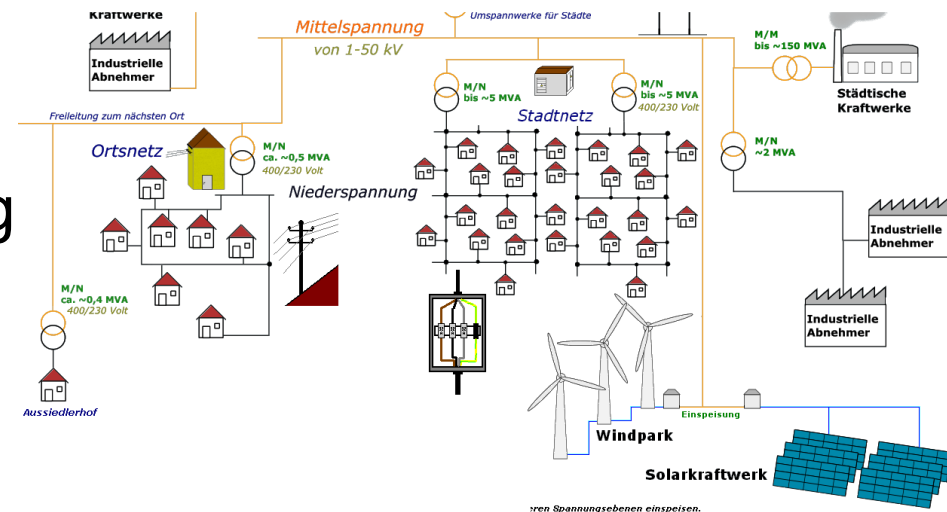
4. Beispiel Domäne Verteilnetz

5. Take Home Message

4. Domäne Verteilnetz

Stromnetz im Nieder- und Mittelspannungsbereich

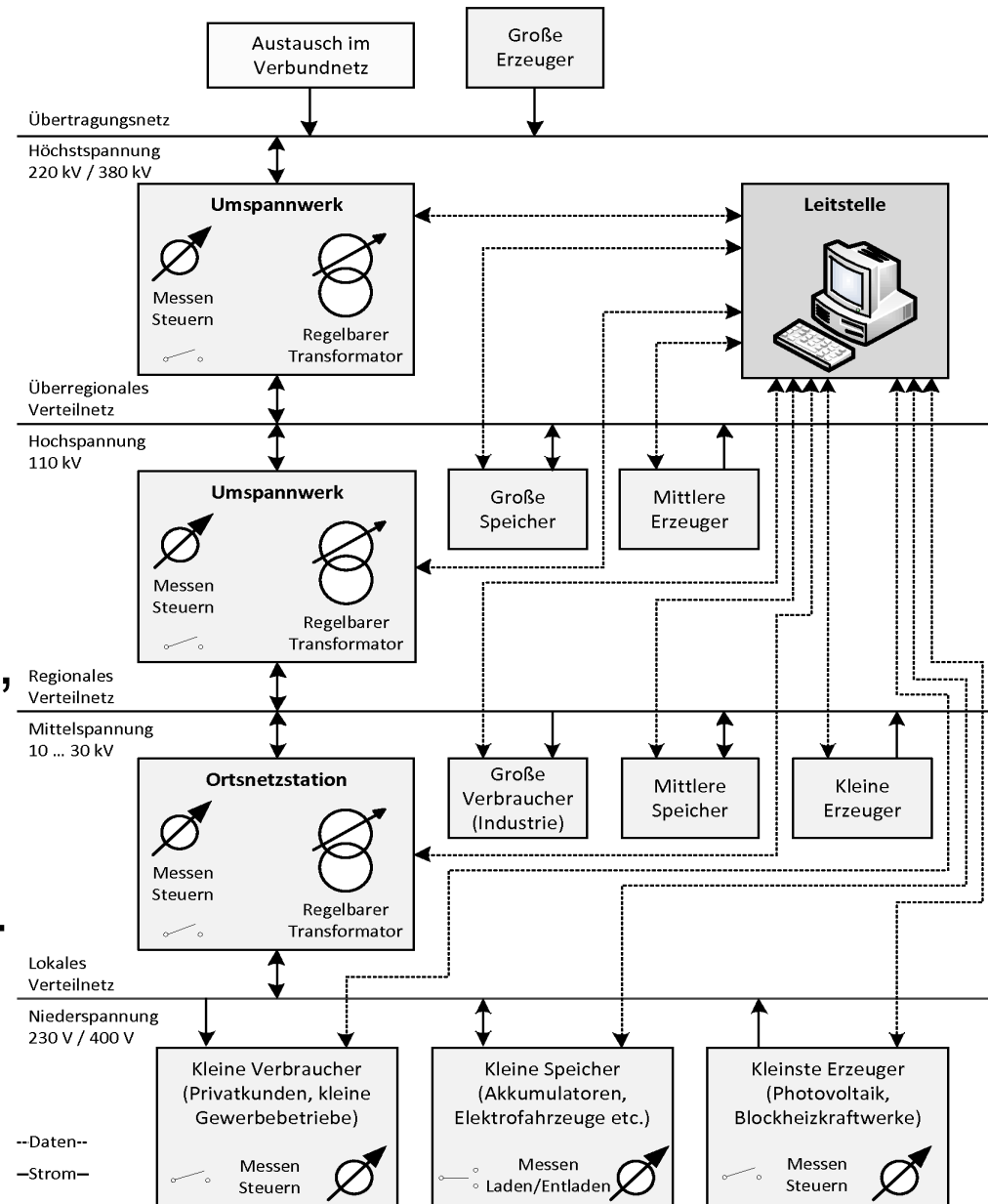
- **Betreiber:** idR lokale Energieversorgungsunternehmen
 - > 720 Stadtwerken, ca. 70 regionalen Netzbetreibern und über 100 private Versorger
- **Niederspannungsnetze**
 - 100m – wenige km
 - sternförmige Versorgung
- **SmartGrid:** Kommunikation zur Lastflusssteuerung, Netzüberwachung, ...



4. Domäne Verteilnetz

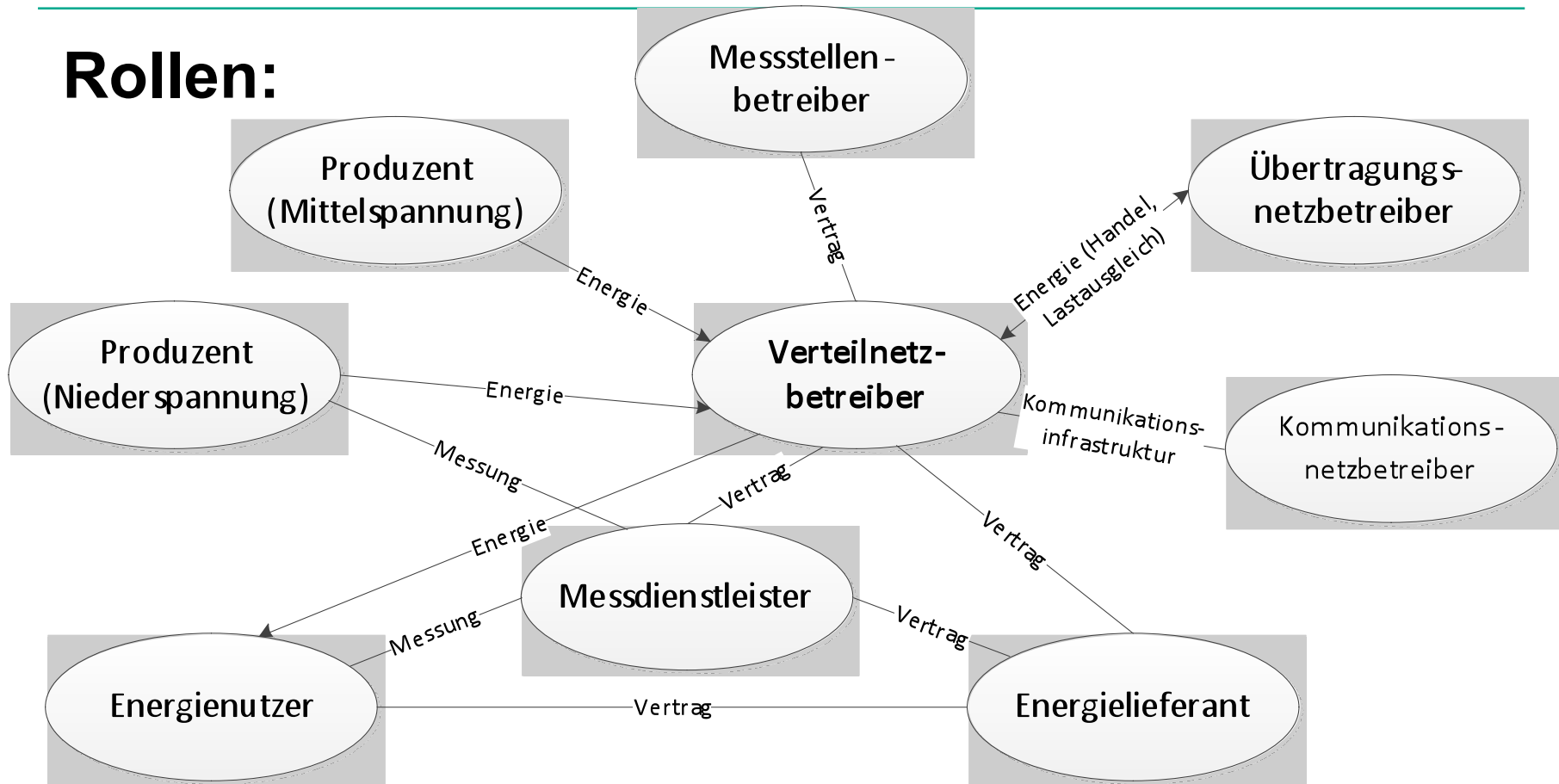
Aktives Verteilnetz

- **Umspannwerke:**
Transformation zw
Spannungsebenen
- **Ortsnetzstationen:**
Transformation Mittel-,
Niederspannetze
- **Erzeuger:**
Windparks, Biogas, ...



4. Domäne Verteilnetz

Rollen:



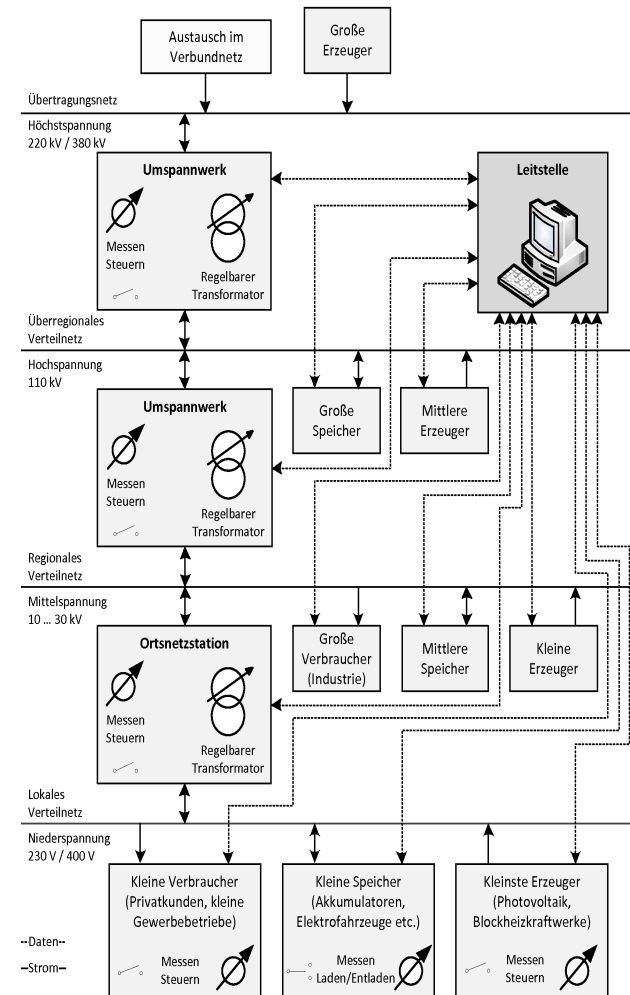
4. Domäne Verteilnetz

Use-Cases u.a.

- Energieeinspeisung
- Steuerung & Überwachung
- Tarifierung

Sicherheitsanforderungen

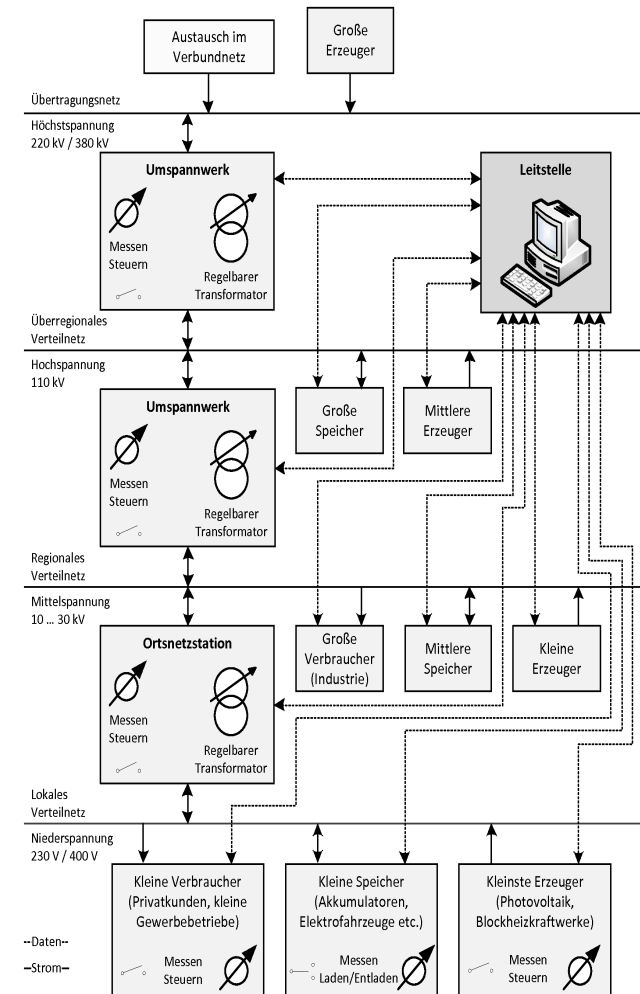
- Rollen-abhängige Pflichten
Steuern, Warten, ...
- Use-case abhängige Daten:
Verbrauchsdaten, Steuerungsdaten



4. Domäne Verteilnetz

Rolle **Energie-Produzent:**

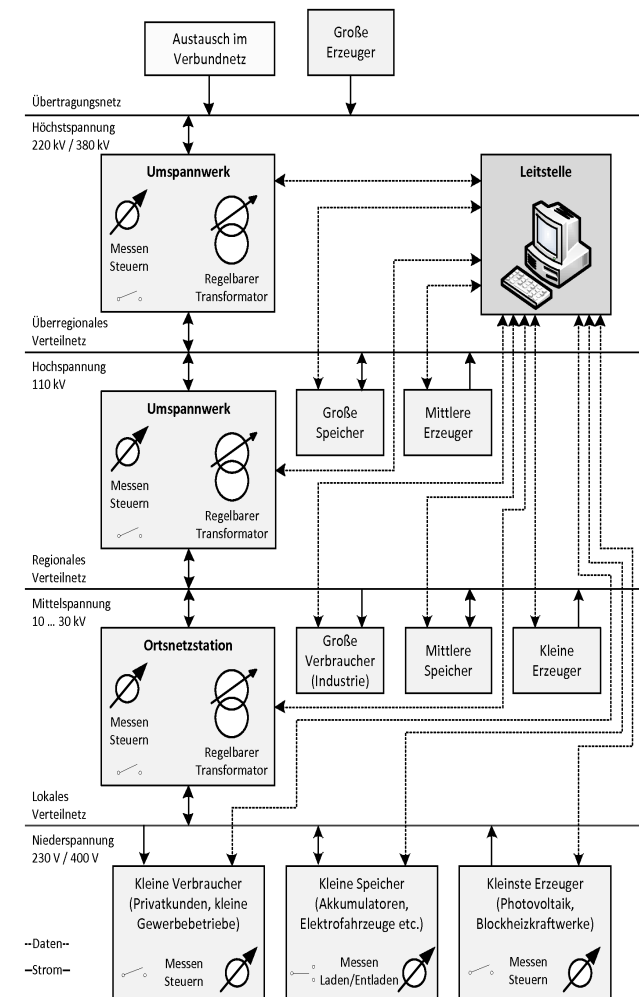
- **Relevante Daten:**
Verbrauch, Abrechnung
- **Anforderungen**
 - **Korrektheit, Zuordenbarkeit** von Messwerten, Prognose- und Abrechnungsdaten
 - **Vertraulichkeit** von Verbrauchswerten



4. Domäne Verteilnetz

Rolle Übertragungsnetzbetreiber

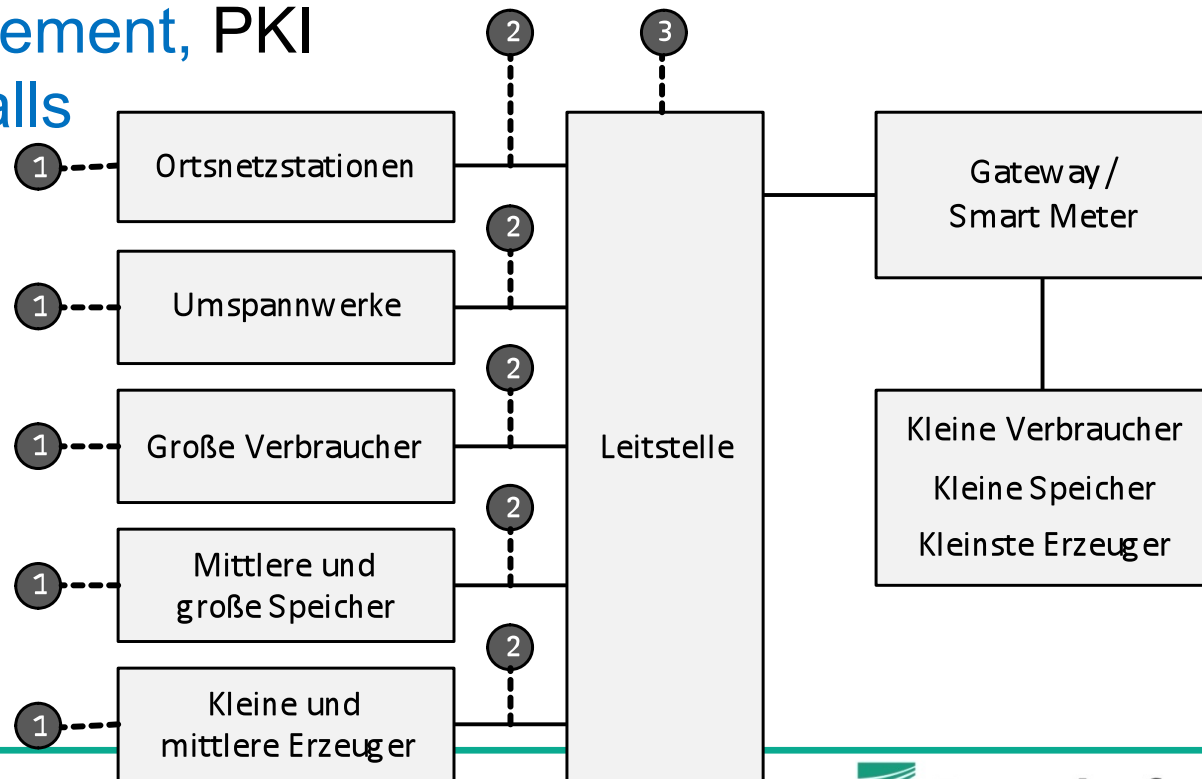
- **Relevante Daten:**
Steuerung, Statusdaten
- **Anforderungen**
 - Verfügbarkeit des Übertragungsnetzes
 - Korrektheit, Zuordenbarkeit, Aktualität von Steuerdaten, Statusdaten



4. Domäne Verteilnetz

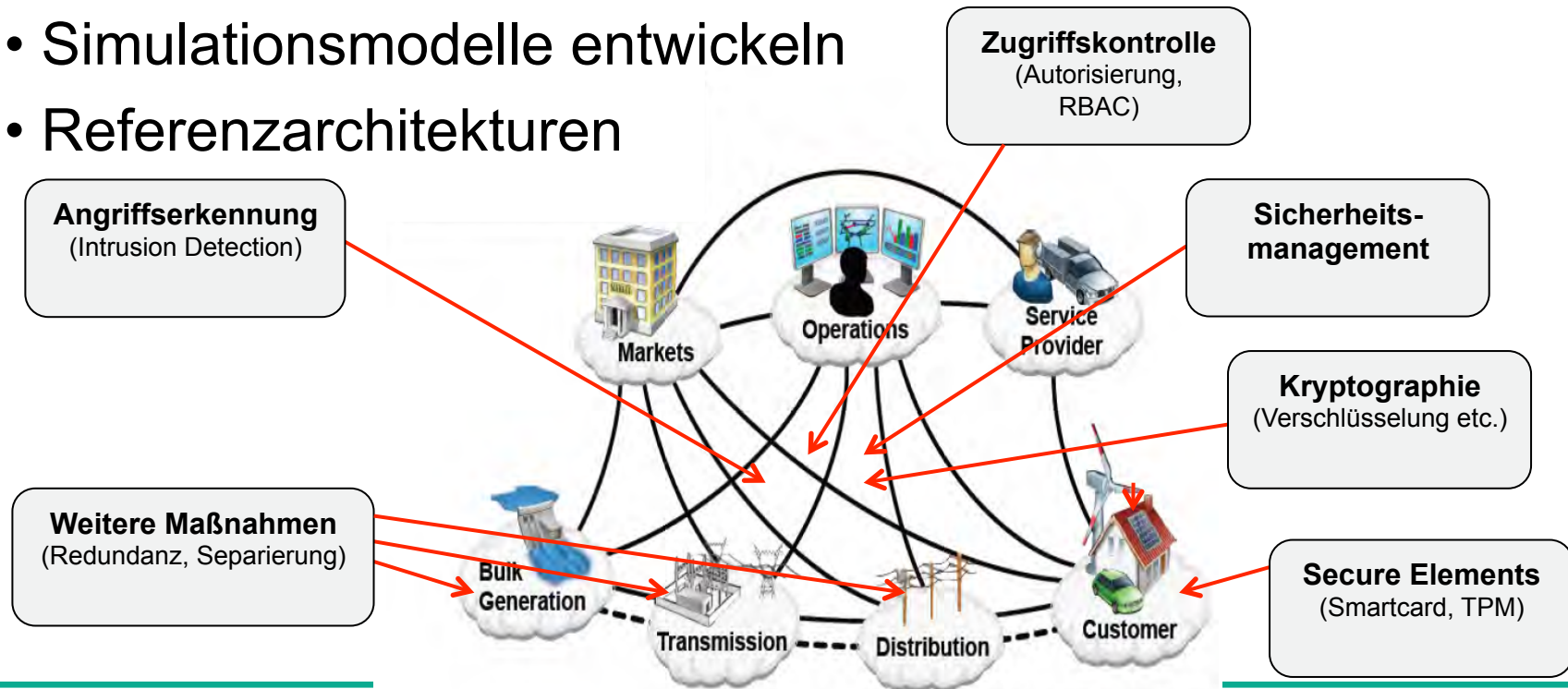
Sicherheits-Architektur & -Konzepte:

- Rollenbasierte Zugriffe: **Zweckgebundene Verarbeitung**
- **Identitätsmanagement, PKI**
- **Spezielle Firewalls**
-



Nächste Schritte

- Schnittstellen und Domänenübergänge spezifizieren
- Durchgehende Bedrohungs- und Risikoanalyse
- Simulationsmodelle entwickeln
- Referenzarchitekturen



Überblick

1. Motivation

IKT als Nervensystem des SmartGrid

2. Domänen-orientierter Ansatz

Teile und Herrsche: Komplexitätsreduktion

3. Domäne Privatkunde

4. Domäne Verteilnetz

5. Take Home Message

Take home Message



IKT ist das Nervensystem des Smart Grid:

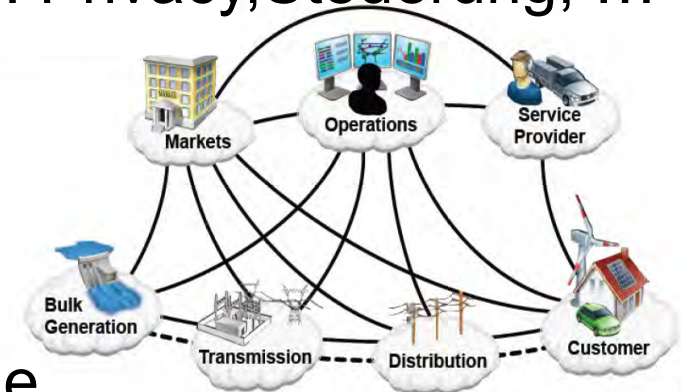
- Smart Grid: **komplexe**, kritische Infrastruktur

Lösungsansatz: Domänen-basiertes Vorgehen

- **Domänen-spezifische** Anforderungen: Privacy, Steuerung, ...
- **Aufgaben-orientierte** Sicherheit
Rollen-Zugriffsrechte, Schlüssel, ...

Nächste Schritte:

- **Sicherheitskonzept** incl. Risikomodelle
- **Simulationsmodelle**, Referenzarchitekturen



Vielen Dank für Ihre Aufmerksamkeit



Claudia Eckert

TU München,

Lehrstuhl für Sicherheit in der Informatik

Fraunhofer AISEC, München



E-Mail: claudia.eckert@sec.in.tum.de

Internet: <http://www.sec.in.tum.de>

<http://www.aisec.fraunhofer.de>