# AP1.5: Sicherheitsmechanismen

Christine Rosinger, Mathias Uslar
OFFIS - Institut für Informatik

## ▶ Forschungsfrage und Kontext


### Problemstellung

- Verteilte Organisation des Stromnetzes erfordert neue Sicherheitskonzepte
- Böswillige Agenten können Vertrauenswürdigkeit in Frage stellen und das System zum Zusammenbruch bringen

### Zielsetzung

- Modellierung eines verteilten Vertrauensmodells für die vertrauenswürdige Verbundbildung
  - Wie sieht der Aufbau des Vertrauensmodells aus?
  - Wie wird das Vertrauensmodell angewendet?

## ▶ Methodik

### Evaluation anhand von Bedrohungsszenarien

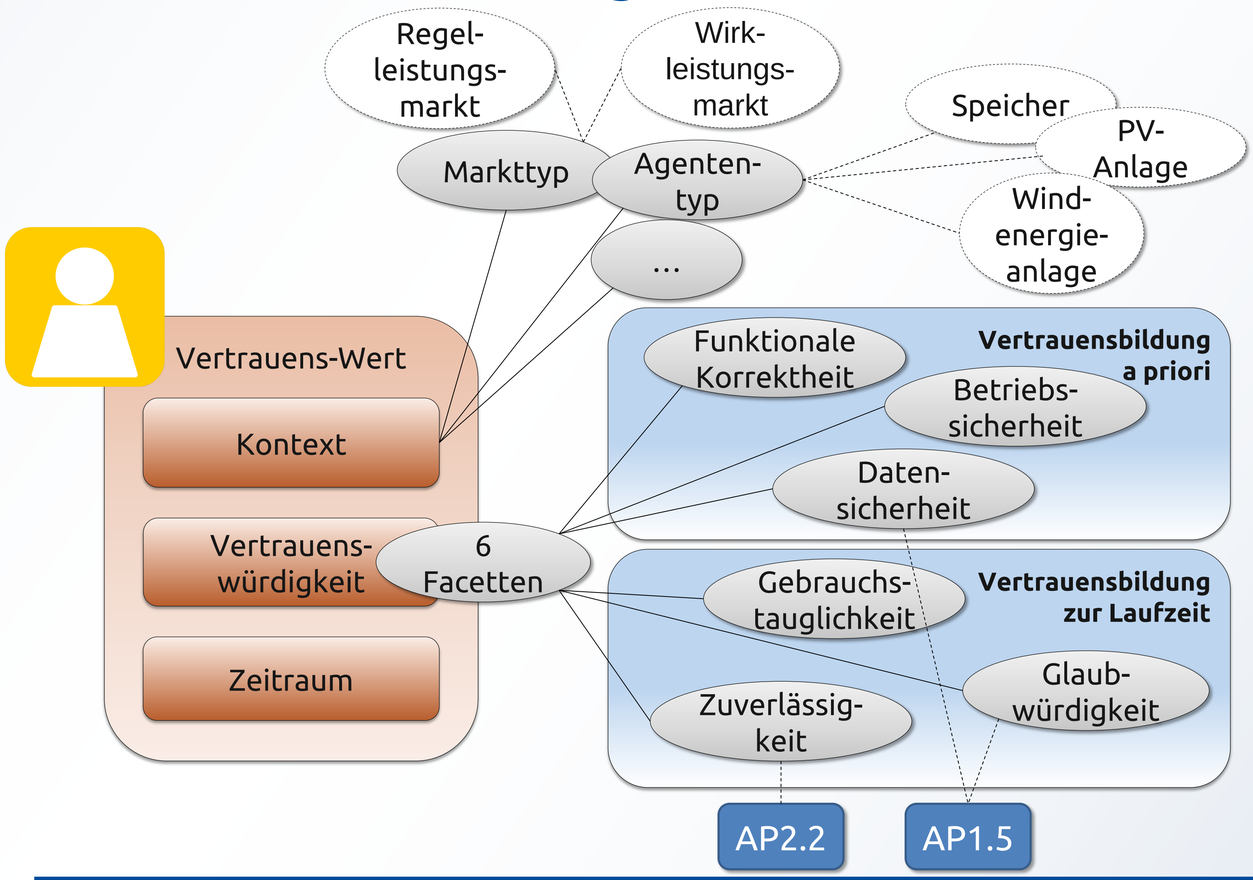
- Mögliche Bedrohungsszenarien
  - BS1: Ein Agent einer Anlage täuscht eine falsche Identität vor. Er gibt vor ein flexibler Speicher zu sein, ist aber eine PV-Anlage. Er kann daher den vorgegebenen Fahrplan nicht erfüllen.
    - Evaluationskriterium: Anzahl der Verbundbildungen, nach denen die Täuschung durch das Vertrauensmodell aufgedeckt wird.
  - BS2: Ein Agent einer Anlage erfüllt seine Fahrpläne unregelmäßig.
  - BS3: Ein Agent einer Anlage widerruft kurz vor Abschluss der Verbundbildung die Teilnahme am Verbund.

## ▶ Erste Ergebnisse

### Vergleich zentrales/dezentrales Modell

| | Vorteil | Nachteil |
|---|---|---|
| Zentral | • Vertrauens-Wert leicht zu überwachen<br>• Fehlerhafte Werte leicht widerrufbar | • Single point of failure, z.B. durch DoS-Angriff<br>• Keine eigene Gewichtung des Vertrauens-Wertes |
| Dezentral | • Eigene Gewichtung des Vertrauens-Wertes möglich<br>• Kompromittierung einzelner Teilsysteme betrifft Gesamtsystem wenig | • Zentrale Kontrollinstanz fehlt<br>• Widerruf fehlerhafter Vertrauens-Werte aufwändig<br>• Höherer Aufwand für Überprüfung der Reputation |

### Entwurf Modellierung Vertrauens-Wert




## ▶ Ausblick und offene Fragen

- Konzeption der Phasen des Vertrauensmodells
- Entwurf von weiteren relevanten Bedrohungsszenarien für die Evaluation, sowie entsprechender Evaluationskriterien, die durch unkooperative Agenten auftreten können
- Identifikation von Sicherheitsanforderungen und einzusetzenden Sicherheitsstandards/-richtlinien
  - Richtige Identitäten/ Sicherstellung der Authentizität
  - IEC 62351
    - Teil 8 – Rollenbasierte Zugriffskontrolle
    - Teil 9 – Schlüsselmanagement
- Integration des Vertrauensmodells in die Gesamtsimulation
  - Festlegen der Schnittstellen

### Phasen des Vertrauensmodells