Task Force „Smart Grids“ zur Sicherheit von Energieverteilnetzen

Norbert Zisky
Physikalisch-Technische Bundesanstalt

Physikalisch-Technische Bundesanstalt Braunschweig und Berlin

1887- 2010

www.ptb.de

Dr. Norbert Zisky

Leiter der AG 8.52
„Datenübertragung und -sicherheit“

Aufgaben

- Entwicklung und Einführung offener Kommunikationskonzepte
- Sicherheitskonzepte und Sicherheitsfragen in der Messtechnik
- Testwerkzeuge für Schnittstellen- und Protokollprüfungen

Inhalt

- Motivation
- Task Force „Smart Grids“
- Ergebnisse/Empfehlungen der Smart Grid EG2
- Ausblick

Normungsbemühungen

EU-Kommission ⇨ Normungsauftrag

- Mandat M/441 an CEN, CENELEC und ETSI (12. März 2009)
  - Smart Meter Co-ordination group (SM-CG)
    Mitglieder: CEN/TCs, FACOGAZ (DVGW), ESMIG (European Smart Metering Industry Group mit Firmen wie Actaris, Landis+Gyr, elster, sensus, ….)

Normungsmandat M/441

- Wichtige Aspekte Mandats :
  Interoperabilität, Zusammenführung von Verbrauchsdaten, Datenschutzes (Integrität und Verschlüsselung)
- Proprietäre Lösungen vs. Normen
  Problem: Jede Branche hat eine oder mehrere eigene Lösungen
- Problem: Unterschiedliche Leistungspotenziale der verschiedenen Messgerätearten:

- → Bekannte Ergebnisse:
  Final Report der SM CG v. Dezember 2009

Situation/Einschätzung 2009

- M/441 wird voraussichtlich nicht im geplanten Zeitrahmen abgeschlossen
- EU Kommission setzt neue Schwerpunkte und installiert neue Arbeitsgruppen mit direkter Kontrolle durch die Kommission

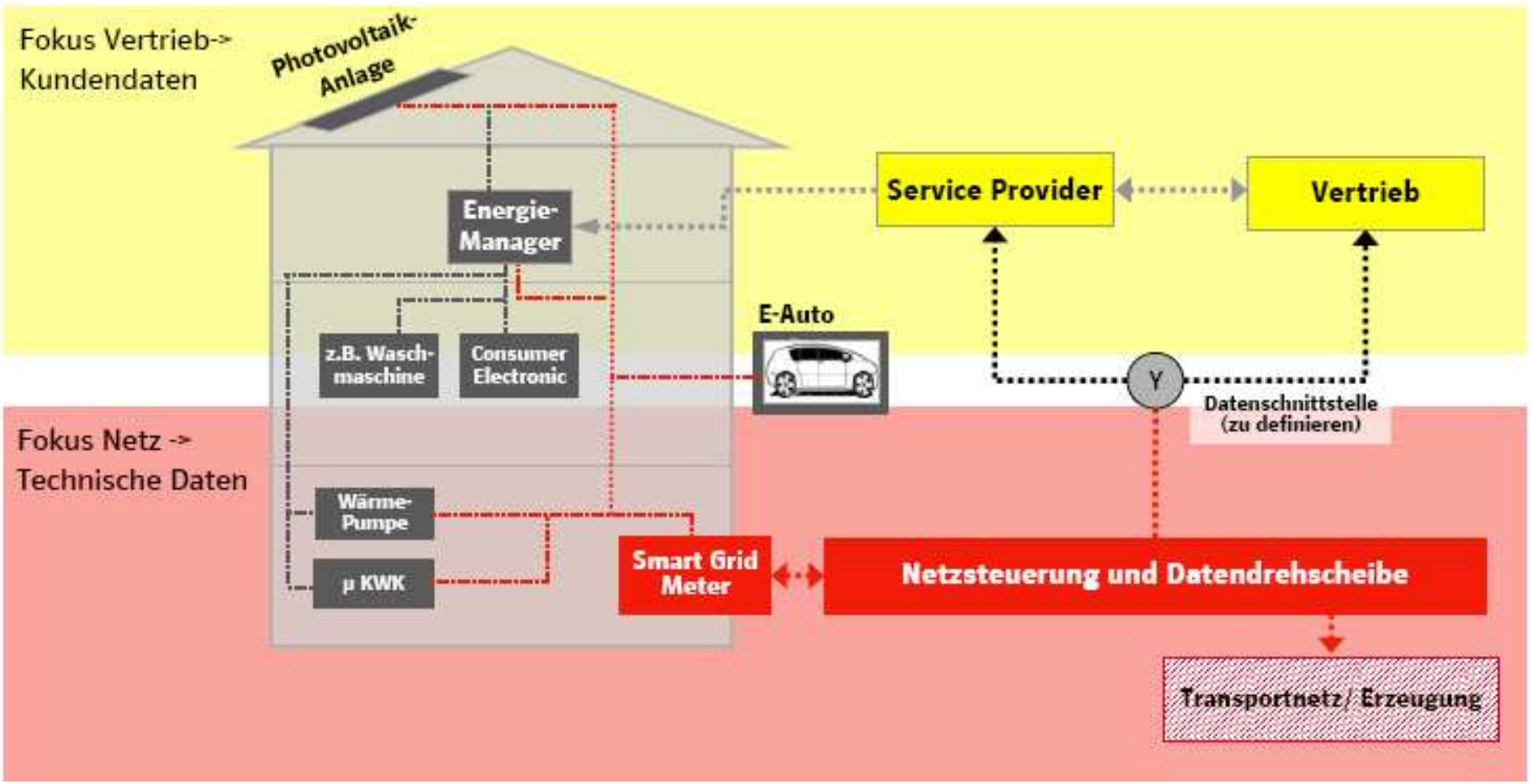
Einführung - Smart Metering→Smart Grids

- Aussage EMATEM 2009:
  Intelligente Zähler - Modebegriff oder Chance
- Kommunizierende Zähler – kein signifikanter Beitrag zur Energieeinsparung erkennbar!??
- Ohne geeignete Messtechnik und Infrastruktur keine Smart Grids
- Netzsteuerung von dezentralen Klein- und Kleinstnetzen

EU Kommissionsentscheidung

- Bildung einer Task Force „Smart Grid“
  Ziel: Erleichterung und Unterstützung der EU-weiten Einführung von Smart Grids
- Mitwirkung aller relevanten Behörden und Interessengruppen
- Lenkungsausschuss bildet drei Expertengruppen
- Alle drei Gruppen entwickeln eine gemeinsame Vision für die Einführung von Smart Grids in Europa
- Identifikation der Regulierungsempfehlungen und zu lösenden Kernfragen

Datenfluss im Smart Grid



Quelle: Dr. J. Kabs, E.ON Energie AG

Task Force Smart Grid - Überblick

Expert Group	1 Functionalities for Smart Grids	2 Regulatory recommendations for data safety, data handling and data protection	3 Roles and responsibilities of actors involved in the Smart Grids deployment
Aufgabe	Regulatorische Funktionen für Smart Grids und Messgeräte	Sicherheit von Daten und Umgang mit Daten, Datenschutz	Rollen und Verantwortlichkeiten aller an Smart Grid beteiligten Akteure
Ergeb-nisse	Funktionalitäten, die Smart Grids und Messgeräte haben sollten	Identifizieren der geeigneten rechtlichen Empfehlungen für die Datenverarbeitung, die Sicherheit und den Verbraucherschutz	Empfehlungen für Zuständigkeiten und Zusammenhänge

Wesentliche Erkenntnisse und Empfehlungen Task Force „Smart Grid“

- Standardisierungen für Smart Grid Produkte & Lösungen sollten bei Entwicklung bereits Datenschutz und Datensicherheit berücksichtigen („Privacy by design“)
- Untersuchung einer technischen Daten
- Klare Definition der Schnittstellen für Datenhaltung
- Die Finanzierung der Datensicherheit in Smart Grids sollte in Form eines adäquaten Modells alle Netznutzer angemessen berücksichtigen
- Notwendigkeit weiterer Studien zum Thema Datenverarbeitung in Smart Grids

Folie wird nachfolgend erweitert und orientiert sich am Report der SG EG2

Sicherheit und Schutz der Daten im Smart Grid verlangen eine Einbindung aller Interessengruppen bei der Definition von Schutzkonzepten und deren Finanzierung

Quelle: Dr. J. Kabs, E.ON Energie AG

Exkurs Sicherheit

- Systemarchitektur
- Schutzziele und Sicherheitsmechanismen
- Schutzziele in der Messtechnik
- Sicherheitsklassen

Von der Idee zur Systemarchitektur

- Kommunikationsanforderungen festlegen
- Sicherheitsanalyse: Systemumfeld, Marktpartner
  heute: stark verändertes Systemumfeld mit neuen Anforderungen
- Sicherheitsziele festlegen
- Sicherheitsstufe festlegen
  Problem: Marktpartner haben unterschiedliche Sicherheitsziele im gleichen Systemumfeld
- Sicherheitskonzept und Systemarchitektur festlegen:

IT-Sicherheit – Schutzziele

Schutzziel	Sicherheitsdienst
Vertraulichkeit (confidentiality)	Verschlüsselung
Unversehrtheit, Integrität (integrity)	Hash, MAC, Signaturen
Herkunft, Echtheit (authenticity)	Signaturen
Nichtabstreitbarkeit (non-repudiation)	Signaturen
Verfügbarkeit (availability)	Techn. Maßnahm., Redundanz
Identifikation (identifikation)	Passwort, challenge response

Schutzziele Messtechnik

Schutzziel	Sicherheitsdienst
Vertraulichkeit (confidentiality)	Verschlüsselung
Unversehrtheit, Integrität (integrity)	**Hash, MAC, Signaturen**
Herkunft, Echtheit (authenticity)	**Signaturen**
Nichtabstreitbarkeit (non-repudiation)	Signaturen
Verfügbarkeit (availability)	Techn. Maßnahm., Redundanz
Identifikation (identifikation)	Passwort, challenge response

→ Einsatz von Signaturen auf der Grundlage asymmetrischer Kryptosysteme für das Messwesen

Stand der Technik für Massenanwendungen

Schutzziele Messtechnik im Wandel

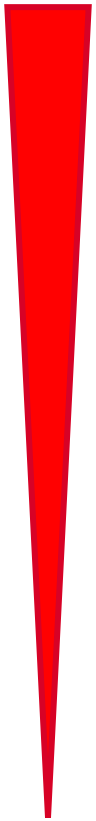
Schutzziel	Sicherheitsdienst
Vertraulichkeit (confidentiality)	Verschlüsselung
Unversehrtheit, Integrität (integrity)	**Hash, MAC, Signaturen**
Herkunft, Echtheit (authenticity)	**Signaturen**
Nichtabstreitbarkeit (non-repudiation)	Signaturen
Verfügbarkeit (availability)	Techn. Maßnahm., Redundanz
Identifikation (identifikation)	Passwort, challenge response

→ Einsatz von Signaturen auf der Grundlage asymmetrischer Kryptosysteme für das Messwesen

Stand der Technik für Massenanwendungen

Security classes

Security



Security classes of cryptographic systems

1. Reliable by information theory

2. Strong cryptographic

3. Well investigated

4. Less investigated

5. Undisclosed („security by obscurity“)

Task Force „Smart Grid“
Executive Summary

- Identifizieren eines angemessenen Regulierungsbedarfs – Empfehlungen für Datenverarbeitung, Sicherheit und Verbraucherschutz
- Begriffsdefinitionen für Smart Grids, z.B. personenbezogene Daten, technische Daten
- Daten mit Personenbezug müssen beim Datenaustausch dem EU Gesetzrahmen hinsichtlich Privatsphäre und Datenschutz entsprechen
- Smart Grid Focus Europa: Energiediebstahl und Privatsphäre vs. Welt (z.B. USA) Energiediebstahl und böswillige Angriffe
- Entwurf von Smart Meter Systemen erfordert strikte Einhaltung der Datenschutzgesetze

Task Force „Smart Grid“
Executive Summary – Fortsetzung 1

- Smart Grids werden positiv bewertet, aber neue Risiken bei Datensicherheit und Vertraulichkeit
- Europäische Verbrauchergruppen verlangen klare Festlegungen für Auslesen und die Nutzung der Daten. Daten dürfen nur mit Zustimmung der Verbraucher gewonnen und ausgewertet werden
- ESOs sollten bei Smart Grid Standards von Beginn an ein angemessenes Niveau von Datenschutz und Sicherheit berücksichtigen
- Abschnitt Datensicherheit: Zusammenfassung existierender Standards, Aufdecken von Lücken/Bedarf bei der Entwicklung von Smart Grids .
  Identifikation verantwortlicher ESOs für jeden Bereich → Standardisierungsbedarf

Task Force „Smart Grid“
Executive Summary – Fortsetzung 2

- SG EG2 identifiziert deutliche Lücken für Smart Grids bei Datenhandling/-sicherheit einerseits und EU Standards andererseits

  Verweis auf Standards, Richtlinien und Code of Practice anderer Bereiche (Banken, Kreditkarten…) mit definiertem Management persönlicher und kartenbezogener Daten
  Vergleich dieser Risiken und Anforderungen mit SG-Ansätzen
  → ggf. Übertragung der Lösungsansätze auf SG

- Gefahr der Definition von Datenstrukturen für bestimmte Nutzergruppen, die gegen Datenschutzfestlegungen und Gesetze verstößt.
  Deshalb Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten

Empfehlungen Task Force „Smart Grid“ EG2
-1-

- Beauftragung SG-EG2 mit
  Bewertung wie Vertraulichkeit und Datenschutz
  bei Smart Metering/Grids mit dem EU-Vertraulichkeit- und
  Datenschutz-Regelwerk abstimmbar sind

  → Ziel: Detaillierter EU Standard
  Sicherheit/Vertraulichkeit für Smart Meter und in Smart Grids

- ESOs sollten bei der Standardisierung Vertraulichkeit und
  Datensicherheit angemessen berücksichtigen

Empfehlungen Task Force „Smart Grid“ EG2 -2- Thema Sicherheit (Security):

- ESOs mit Update, Erweiterung oder Entwicklung neuer Standards beauftragen; Sicherheitsaspekte von SG basierend auf EU-Anforderungen berücksichtigen

  ESOs sollten vor Start der Standardisierung SG EG-Empfehlungen und die relevanten Standards berücksichtigen sowie Veränderungen, Zusätze und erforderliche zukünftige Arbeit ergänzen

  ESOs sollten den Stand kryptographischer Dienste evaluieren und die passenden Technologien in die Standards integrieren

  - Kein Ausschluss der Erstanwendung symmetrischer Kryptographie mit dem nachträglichen sanften Übergang zu asymmetrischen Verfahren
  - Untersuchung von Geschäftsmodellen für Aufbau und Unterhalt von Certification Authorities
  - Studie über multinationales Schlüsselmanagement (z.B. EU-CA für Messgeräte)

Empfehlungen Task Force „Smart Grid“ EG2
-3- Thema Datenverarbeitung

- Bedarf an weiteren Pilotinstallationen für Datenverarbeitungssysteme, Ziel ist eine Bereitstellung leistungsfähiger Verfahren/Prinzipien für Smart Grids, Konsultation Bank- und Kreditkartenindustrie

  Zusammengefasste Ergebnisse sollen den ESOs als Bericht übergeben werden,
  Ziel: Hervorheben des zusätzlichen Standardisierungsbedarfs auf diesem Gebiet

Empfehlungen Task Force „Smart Grid“ EG2
-4- Vertraulichkeit:

- Trennung von Kundendaten (Rückführung auf einen individuellen Verbraucher) und technischen Daten (aggregierte und anonyme Daten ohne explizite Referenzen auf Personen)
  → Verbesserung des Schutzes persönlicher Daten

  Klare Definition der Rollen und Verantwortlichkeiten und deren Schnittstellen für Datennutzung
  (Eigentum, Datenbesitz und -zugriff, Schreib-/Leserechte)

  SG EG2 sollte damit beauftragt werden, relevante Details (Datenelemente, Rollen, Verantwortlichkeiten , Besitz, Zugriff herauszuarbeiten

  Erarbeiten abgestimmter Modelle wie Verbraucher die Verwendung eigener Daten kontrollieren können

  Methoden zur wirkungsvollen Überwachung und Durchsetzung von Datenschutz- und Vertraulichkeitsregeln

Task Force Smart Grid - Reports

Expert Group	1 Functionalities for Smart Grids	2 Regulatory recommendations ..	3 Roles and responsibilities ..
Draft reports	expert_group1.pdf	expert_group2.pdf	expert_group3.pdf

Weitere Details unter:

http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

Ausblick

- Betrieb, Steuerung und Unterhalt von Smart Grids stellen hohe Anforderungen an alle Beteiligten
- Sicherheitsfragen: Datensicherheit und vor allem Datenschutz sind zentrale Schwerpunktthemen in Energienetzen
- Arbeiten der Task Force SG-EG2 werden weitergeführt, wenn die Empfehlungen von der Kommission angenommen werden

Aktuelle News

Einladung: [SG-EG2] Phase 2 Kick-Off
Di 28.09.2010 13:00 - 14:30 (Wiederholend)
Teilnahme ist erforderlich für Norbert Zisky
Leitung: Michael.John@elster.com

Ort:
MeetMe Bridge Access Code 72566572, Dial-ins inline

Dear all,
on behalf of Frank Hyldmar, I would like to invite to a kick-off call for the second phase of the Expert Group work in order to outline scope and time lines of new deliverables and to discuss the next steps.

Best regards,
Michael
-
Michael John

Ausblick

- Betrieb, Steuerung und Unterhalt von Smart Grids stellen hohe Anforderungen an alle Beteiligten
- Sicherheitsfragen: Datensicherheit und vor allem Datenschutz sind zentrale Schwerpunktthemen in Energienetzen
- **Arbeiten der Task Force SG-EG2 werden weitergeführt!!**

Sicherheit und Schutz der Daten im Smart Grid verlangen eine Einbindung aller Interessengruppen zur Festlegung von Schutzkonzepten und eine faire Finanzierung des Aufwands

Vielen Dank!

- Sehen Sie Bedarf, bestimmte Fragen/Probleme zur Vertraulichkeit/Sicherheit für den Bereich Wärmemengenmessung/Durchflussmessung in der Task force SG-EG2 zu behandeln?
- Gibt es Überlegungen zu Schutzzielen für diesen Bereich?