Datenmodelle zur Sicherung des metrologischen Blocks

Norbert Zisky
Physikalisch-Technische Bundesanstalt

Inhalt

- Einführung
- Metrologischer Block
- Sicherheitslösungen und Kommunikation
- Zusammenfassung

Einführung: Motivation

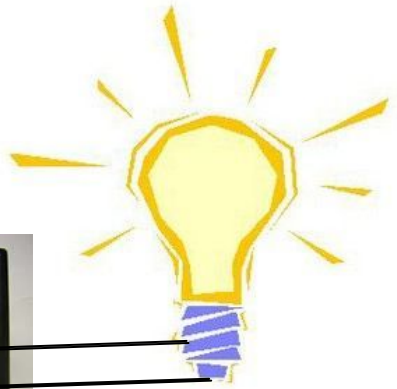
- Verstärkte Beschäftigung mit Sicherheitsfragen seit 2001
- Sicherheitsbewusstsein im Messwesen ist in den zurückliegenden Jahren gewachsen
- PTB war an mehreren Projekten beteiligt:
  SELMA, SIMEDAKO, INSIKA
- Verschiedene Konzepte entwickelt und umgesetzt
- Schlüsselprojekt SELMA
  Ziele:
  - Sicherheits-Datenmodell für Verbrauchsmessgeräte
  - Sicherheitsfunktionen (Parametrierung, Fernbedienung)

Einführung: Aktuelle Lage

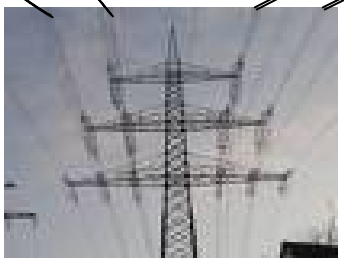
- Trends Kommunikation und Sicherheit:
  - Herstellerspezifische Einzellösungen
  - Konsortiallösungen einzelner Branchen
- Gründe mitunter plausibel
  verändertes Systemumfeld, Verunsicherung
  spezielle Firmeninteressen der Anwender und Hersteller von Messgeräten und Zusatzeinrichtungen
- International:
  sehr unterschiedliches Vorgehen
  klare staatliche Regelungen/Vorgaben vs.
  vollständig liberales Messwesen

„Schöne“ alte Welt

Messdaten



Rechnung



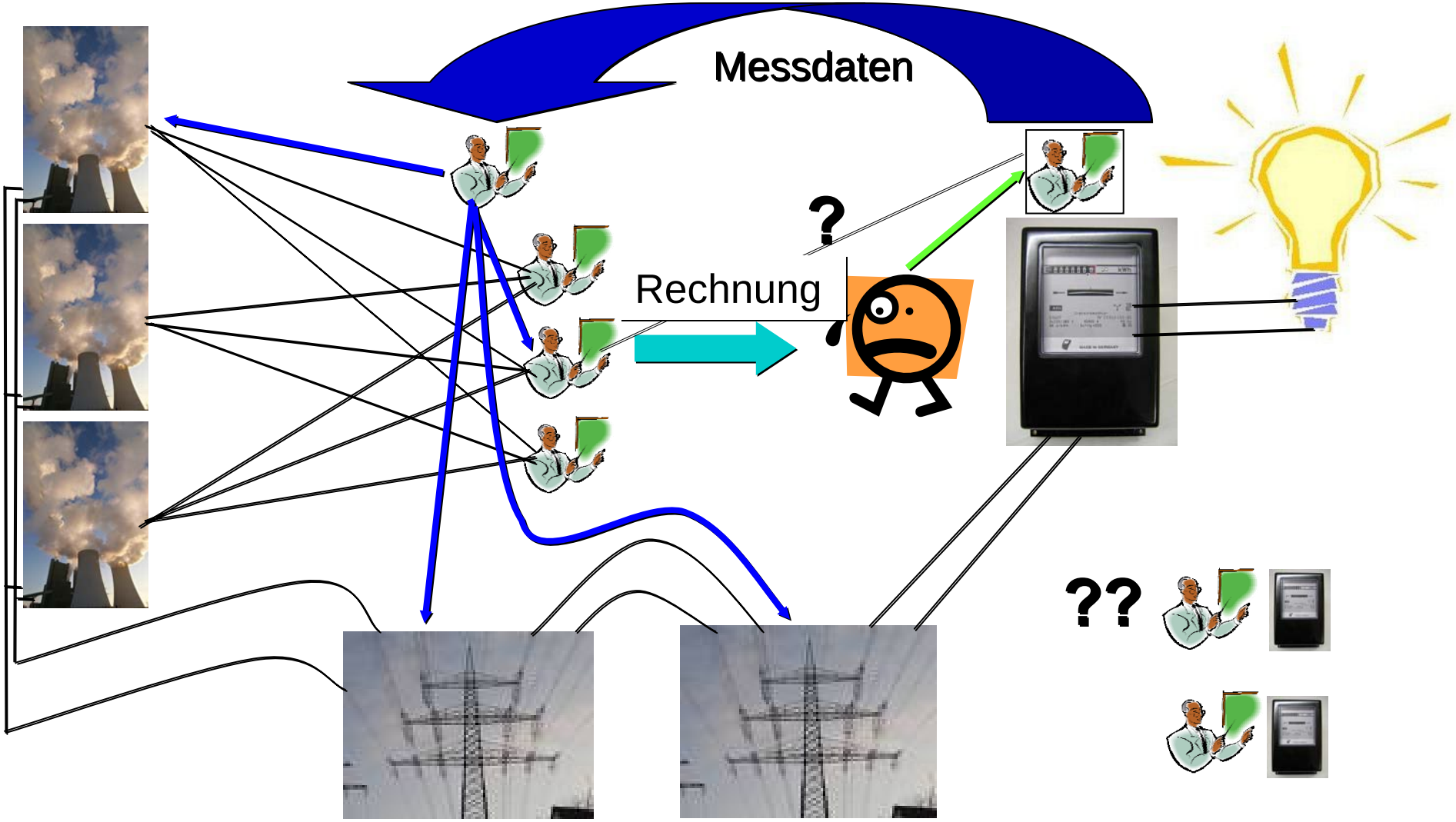
Aber - Das ist nur ¼ der Daten!!!!

Und heute??

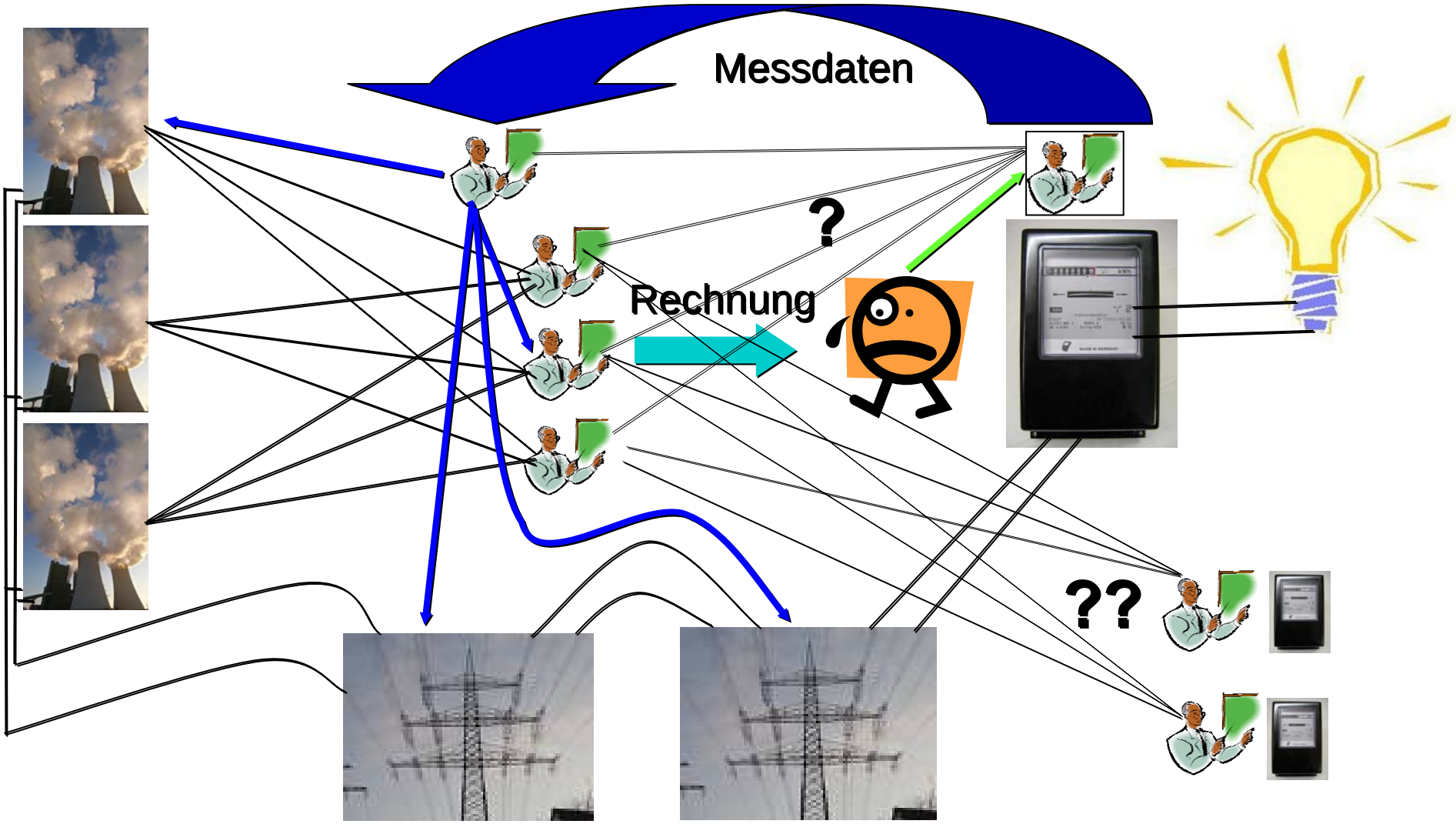
Das war bei Vortrag ein schwarzer Kasten

(aber es soll Tinte gespart werden)

Und heute?? – Der Kunde hat die Wahl



Und heute?? – Einfache Wechselbeziehungen



Einführung: Kernprobleme

- Messtechnik, Kommunikation und Sicherheitstechnik
- Datenschutz, Datenbevorratung, Datenverwendung, wem gehören die Daten
- Neues Systemumfeld, neue Architekturen, neue Tarifmodelle, neue Netzsteuerungsmodelle
- Energieverbrauch für Kommunikation
- Messrichtigkeit und Tarifierung
  Abgrenzung: Verbrauchsmessgeräte E,G,W,W
  E: 42 Millionen Ferraris gegen elektronische fernauslesbare Zähler→ Folgen??

Einführung: Messtechnik und Kommunikation

- Messtechnik, Kommunikations- und Sicherheitstechnik sind heute noch keine Einheit
- Vielzahl Kommunikations-Lösungen: IEC 61107 (1107), M-Bus, LON, DSfG, dlms, CAN, ….
  Stichworte: Anforderungen, Leistungsfähigkeit , Echtzeit, Kommunikationsanforderungen, Kommunikationsmöglichkeiten, Kosten, Sicherheit
- Positive Lösungsansätze für Mindestanforderungen für die Messdatenbereitstellung: MeteringCode des BDEW

Normungsbemühungen

- Proprietäre Lösungen vs. Normen
  Problem: Jede Branche hat eine oder mehrere eigene Lösungen

Ausgewählte Normen Datenübertragung

- Elektroenergieversorgung IEC 61850 (Leit- und Automatisierungstechnik), IEC 60870 oder IEC 62056-21, -42, 46, -53 (dlms) Messung elektrischer Energie - Zählerstandsübertragung, Tarif- und Laststeuerung
- CEN/TC 294 „Kommunikationssyst. für Zähler und deren Fernablesung“ DIN EN 13757 (Physical, Link und Spezieller Application Layer, Zählerauslesung über Funk, Weitervermittlung, Lokales Bussystem
- DIN EN 1434-3 Wärmezähler-Teil 3: Datenaustausch und Schnittstellen
- E DIN 43863-4:2006-09 Zählerdatenkommunikation - IP-Telemetrie, DIN EN 61334-XX-YY Verteilungsautomatisierung mit Hilfe von Trägersystemen auf Verteilungsleitungen (DKE/AK 461.0.14 „Datenübertragung“)
- IEC-Norm: SML – Smart Message Language (in Vorbereitung)
- …….

Normungsbemühungen

- Proprietäre Lösungen vs. Normen
  Problem: Jede Branche hat eine oder mehrere eigene Lösungen
- **Problem: Unterschiedliches Leistungsvermögen der verschiedenen Messgerätearten:**
  einfache, batteriegestützte Einchip-Zähler bis hochkomplexe Messsysteme
- Normungsauftrages der EU-Kommission an die ESO (CEN, CENELEC, ETSI):
  Interoperabilität, Zusammenführung von Verbrauchsdaten, Datenschutzes (Integrität und Verschlüsselung)

EU-Kommission ⇨ Normungsauftrag

- Ziel: Schaffung europäischer Normen mit Interoperabilität von Verbrauchszählern (Wasser, Gas, Elektrizität, Wärme)
  - Darstellung des tatsächlichen (aktuellen) Verbrauchs
  - Rechtzeitige Anpassung der Nachfrage bei Versorgern
  - **Entwicklung genormter Schnittstellen und Datenaustauschformate für sichere bidirektionale Kommunikation**
  - **Flexible Architektur (einfachste bis komplexe Anwendungen)**
  - **Kommunikationsschnittstelle muss geschützten messtechnischen Block übertragen**
  - Berücksichtigung bestehender nationaler und internationaler Normen
- Ausführung: sehr ambitioniert, EU-Normvorlage innerhalb von 9 Monaten!!

Einführung: Messtechnik und Kommunikation

- Messtechnik im Wandel
- Neue Wege in der Kommunikation
- Sicherheit: sichere Messwerte, sichere Bedienung/Parametrierung, sichere Messgeräte
- Leistungsfähigkeit, Energieverbrauch, Kosten (Gesamtbuget)
- Datenbedarf: Jeder Marktpartner hat einen anderen Datenbedarf

Einführung: PTB-Ziele

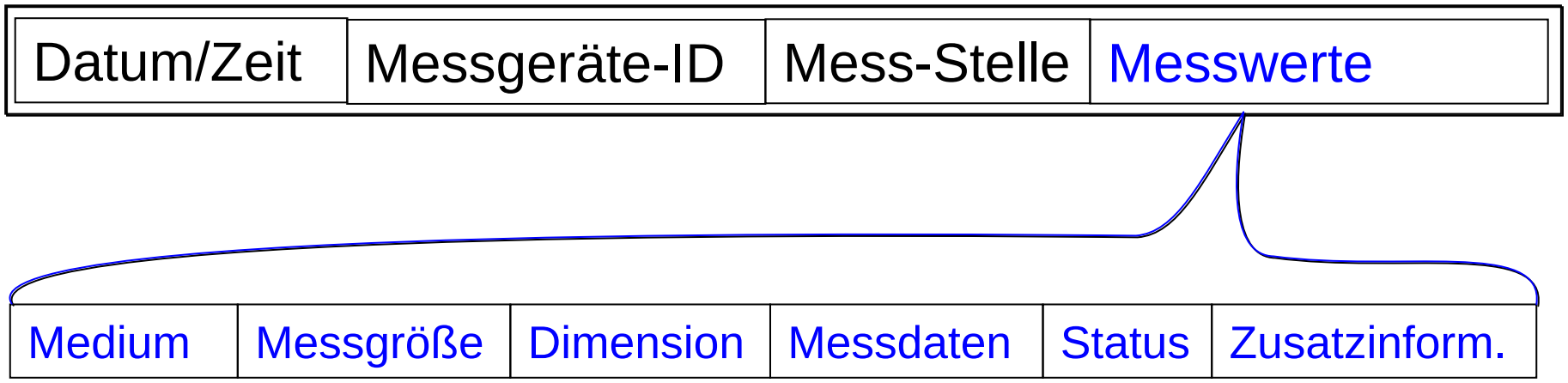
- Schutz des metrologischen Blocks/der Messwerte vor Manipulation
- Gewährleistung der Rückverfolgbarkeit der Messwerte/der Überprüfbarkeit der Rechnung

Was ist ein metrologischer Block?

- Verwendung bestimmt benötigte Daten
- Rechnung für Kunden
- Verrechnung mit anderen Marktpartnern (Lieferant, Netznutzung…)
- Netzsteuerung

Was ist ein metrologischer Block?

- Bestandteile eines Messdatensatzes



Beispiel OBIS-Kennzahle [MeteringCode 2006, Ausg. 2008]:

Medium	Kanal	Messgröße	Messart	Tarif	Vorwert	Messdaten

Messdaten

- Welche Daten, wann, für wen (und zu welchem Preis?)

Jahresablesung E-Zähler: 1 Messdatensatz

Datum	Messgeräte-ID	Mess-Stelle	Ablesewert

Tagesablesung E-Zähler – Lastgang: 96 Messdatensätze

1.01.09/00:15	MG-ID01	4711	1-	1:	1.	29.	1	4734.653	8000
1.01.09/00:30	MG-ID01	4711	1-	1:	1.	29.	1	4734.653	8000
⋮									
2.01.09/00:00	MG-ID01	4711	1-	1:	1.	29.	1	4734.653	8000

Wirkenergie +A

Messdatenvolumen (1)

Jahresablesung E-Zähler: 1 Messdatensatz

Datum	Messgeräte-ID	Mess-Stelle	Ables

≈ 100 byte

Tagesablesung E-Zähler – Lastgang: 96 Messdatensätze

1.01.09/00:15	MG-ID01	4711	1-	1:	1.	29.	1	4734.653	8000
1.01.09/00:30	MG-ID01	4711	1-	1:	1.	29.	1	4734.653	8000
⋮									
2.01.09/00:00	MG-ID01	4711	1-	1:	1.	29.	1	4734.653	8000

Wirkenergie +A

≈ 10000 byte

Messdatenvolumen (2)

Jahresablesung 1 E-Zähler:		Jahresablesung 42 Millionen E-Zähler:
≈ 100 byte	Lastprofil	≈ 4 Gigabyte
≈ 3 Megabyte	Lastgang nur +A	≈ 125 Terabyte
		≈ 125 Billionen (10^{12})

Nur ein Medium!!!

Abrechnungsrelevante Messwerte

- Anzeige am Messgerät oder an der Zusatzeinrichtung
  d.h. beim Verbraucher
  → duplizierte, z.B. für die Rechnungsstellung in einer Zentrale benötigte Messwerte unterliegen dann nicht der Eichpflicht

oder

- Bei Fernauslesung Übertragung mittels eichtechnischer Sicherung mit hohen Sicherheitsanforderungen (Authentizität, Integrität)

- Nachträgliche Tarifierung ohne Bezug auf rückgeführte Messwerte ist nicht gestattet

Schutz des metrologischen Blocks

- Frage: Messdaten am Messgerät = Messdaten der Rechnung

- Verifikationsmöglichkeiten:
  Vergleich Rechnungsdaten mit Messgerätedaten (durch Kunden)
  Einsatz technischer Verfahren: Passwortschutz, CRC, Hash, Verschlüsselung, Signierung
- Passwort: Prinzipiell vorstellbar, aber schwierig umsetzbar, unsicher
- CRC, Hash: nur Schutz gegen passive Gefährdung, kein Schutz gegen aktive Angriffe
- Verschlüsselung: sicheres Verfahren, sehr aufwendige Schlüsselverwaltung oder hohe Gefährdung bei Verwendung von nur einem Schlüssel
- Signierung: sicheres Verfahren, weit verbreitet, Aufwand für Infrastruktur

Kommunikation und Sicherheit

- Primäres Ziel – Grundanforderung neu:
  Daten sollen vom Messgerät zum Datenverwender übertragen werden
- Sekundäres Ziel – Ja, aber!! - Zusatzanforderungen:
  Schnell, zuverlässig, sicher, ……..

Und schon ist man in der Welt der IT-Sicherheit

- Oft Suche nach schnellen Lösungen
  - eigene Protokolle
  - einfache Sicherung CRC16 und Passwort, …..
- meist Nachbesserungen erforderlich

Von der Idee zur Systemarchitektur

- Kommunikationsanforderungen festlegen
- Sicherheitsanalyse: Systemumfeld, Marktpartner
  heute: stark verändertes Systemumfeld mit neuen Anforderungen
- Sicherheitsziele festlegen: z.B. Forderung von Integrität, Authentizität, Vertraulichkeit
- Sicherheitsstufe festlegen
- Problem: Marktpartner haben unterschiedliche Sicherheitsziele im gleichen Systemumfeld
- Systemumfeld Verbrauchmessgeräte im Wandel
- 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 (identification)	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 (identification)	Passwort, challenge response

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

Stand der Technik für Massenanwendungen

Messdaten mit Signatur

Messdatensatz ohne Signatur

Datum	Messgeräte-ID	Mess-Stelle	Ablesewert
30.11.2009	xyz987654321012345	zyx0123456789	22567

Messdatensatz mit Signatur

Datum	Messgeräte-ID	Mess-Stelle	Ablesewert	Signatur
30.11.2009	xyz987654321012345	zyx0123456789	22567	F2CBD6…7AC2B

Starkes Verfahren:
48 byte (2*24)

F2CBD6A4E4B9AAEA992CF0CBB27A905BBFF3F8B32757AC2B
CC2529BC77208308EC5FCF3BCE6CCE3FDECB0927936062E0

Signatur und Verifikation

1. Messdatensatz muss bei der Prüfung immer bitgenau mit dem Original übereinstimmen

30.11.2009	xyz987654321012345	zyx0123456789	22567	F2CBD6…7AC2B

ca. 800 bit

→ Nach der Datenübertragung muss der originale Datensatz aus den Daten rekonstruiert werden können

2. Prüfschlüssel muss dem Empfänger bekannt sein

3. Empfänger muss sich über die Gültigkeit des Prüfschlüssels informieren können

Technik steht seit Jahren im IT-Bereich zur Verfügung

Datenmodelle festlegen

- Syntax und Semantik für Messdatensätze und Signaturen definieren
  - alle Datenobjekte sollten einzeln identifizierbar sein, OBIS-Kennzahlen gutes Beispiel
  - gute Erfahrungen mit Codierungen mit Basic Encoding Rules (BER), auch Standard in der Sicherheitstechnik,
  - Aufbau hierarchischer Datenobjekte möglich

- Datenverifikation auf der Grundlage einheitlicher Datenmodelle definieren,
  z.B. XML-Strukturen mit allen, zur Verifikation erforderlichen Datenobjekten

- Verfahren wurden erfolgreich getestet: SELMA und INSIKA

Marktaufsicht und Kryptographie

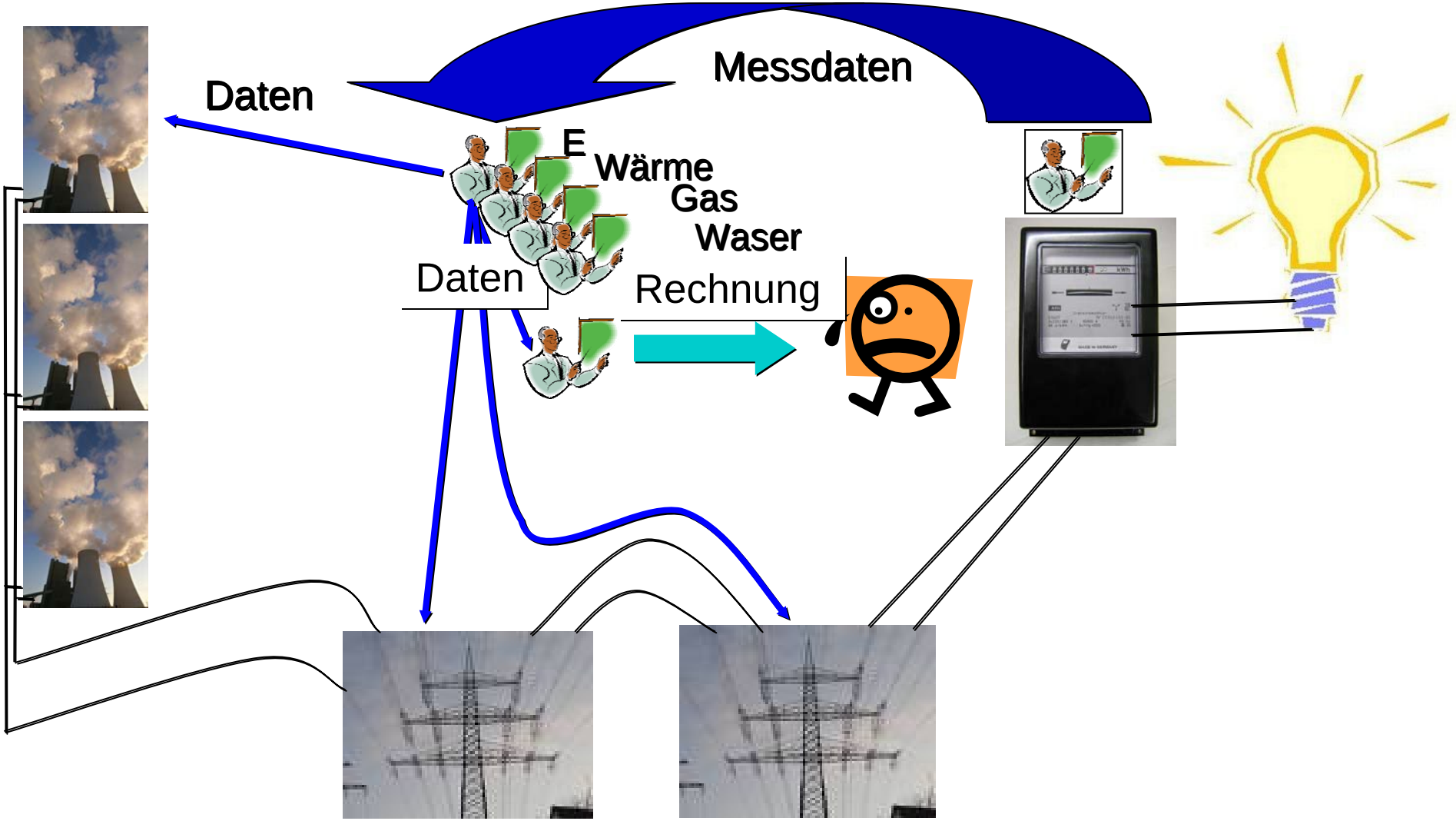
- Lösungsansatz 1- Unsignierte Messdaten: Verifikation von Messdaten durch Vergleich Rechnungsdaten – Datenablesung am Messgerät
  - Messgerät kann manipuliert sein, Kunde müsste mindestens Eichplomben prüfen
  - Ablesefehler insbesondere bei Lastgangzählern wahrscheinlich

  → Hotline o.ä. erforderlich
- Lösungsansatz 2 – Signierte Messdaten: Verifikation von Messdaten unter Verwendung geprüfter Verifikationssoftware nach Datenfernübertragung

Beide Lösungsansätze benötigen eine Marktaufsicht

- Manipulationen direkt am Messgerät unter Bruch der eichtechnischen Sicherung o.ä. sind möglich
- Einsatz von Kryptographie bedeutet nicht absolute Sicherheit!!

Fiktion



Zusammenfassung

- Heute nicht behandelt:
  - kryptographische Zusammenhänge
  - bidirektionale sichere Kommunikation
  - sichere Parametrierung und Downloadkonzepte
  - Zertifikatsverwaltung in PKI-Systemen
  - Analyse vorhandener Systeme

Zusammenfassung

- Kommunikative Zähler im Verbund mit hochkomplexen IT-Systemen erfordern völlig neue Lösungsansätze für das Systemumfeld
- Kommunikation hat ihren Preis
- Sicherheit hat ihren Preis
- Synergien aus Messwesen und Sicherheitstechnik für spartenübergreifende Lösungsansätze nutzen
- Europäische Normungsbemühungen könnten zu verbindlichen Standards führen

Elektronische Signaturen, Technik der Zukunft

- Die europaische Standardisierung bietet Chancen, die wir nutzen müssen
- Die gesetzlichen Grundlagen sind vorgegeben und einzuhalten
- Offene Fragen brauchen Antworten, sie dürfen uns aber nicht daran hindern, die Antworten auch zu suchen
- Die elektronische Welt ist wirklich, es gibt keinen Weg zurück

Quelle:
Elektronische Signaturen, Technik der Zukunft
Ernst-G. Giessmann
T-Systems GmbH, ITC Security, 2003

Vielen Dank!