

Informationstag "IT-Sicherheit im Smart Grid"

Berlin, 23.05.2012

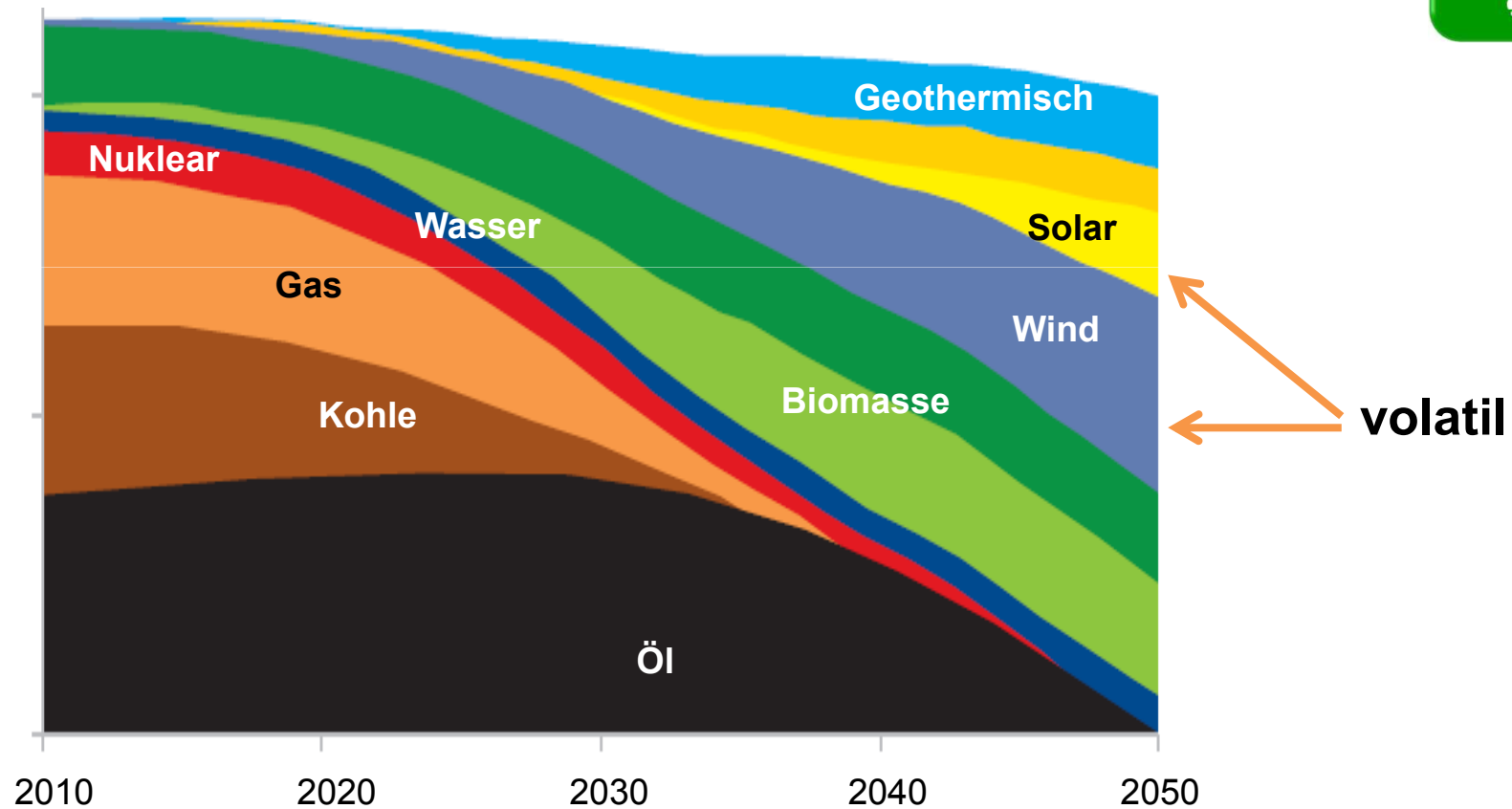
Sicheres Energiemanagement

der nächste Schritt nach dem Smart Meter Gateway

Markus Bartsch



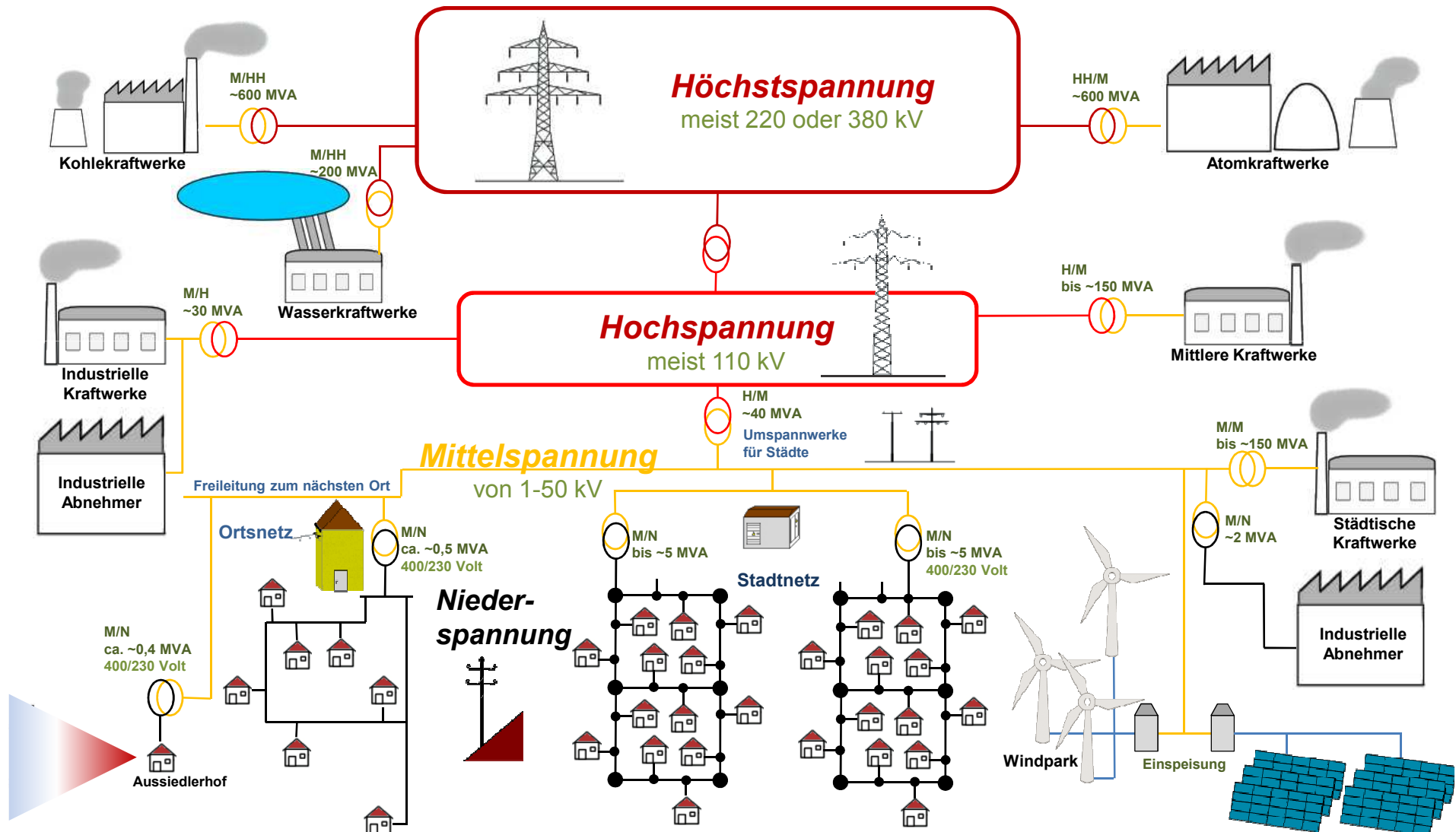
Zukünftige Energiequellen



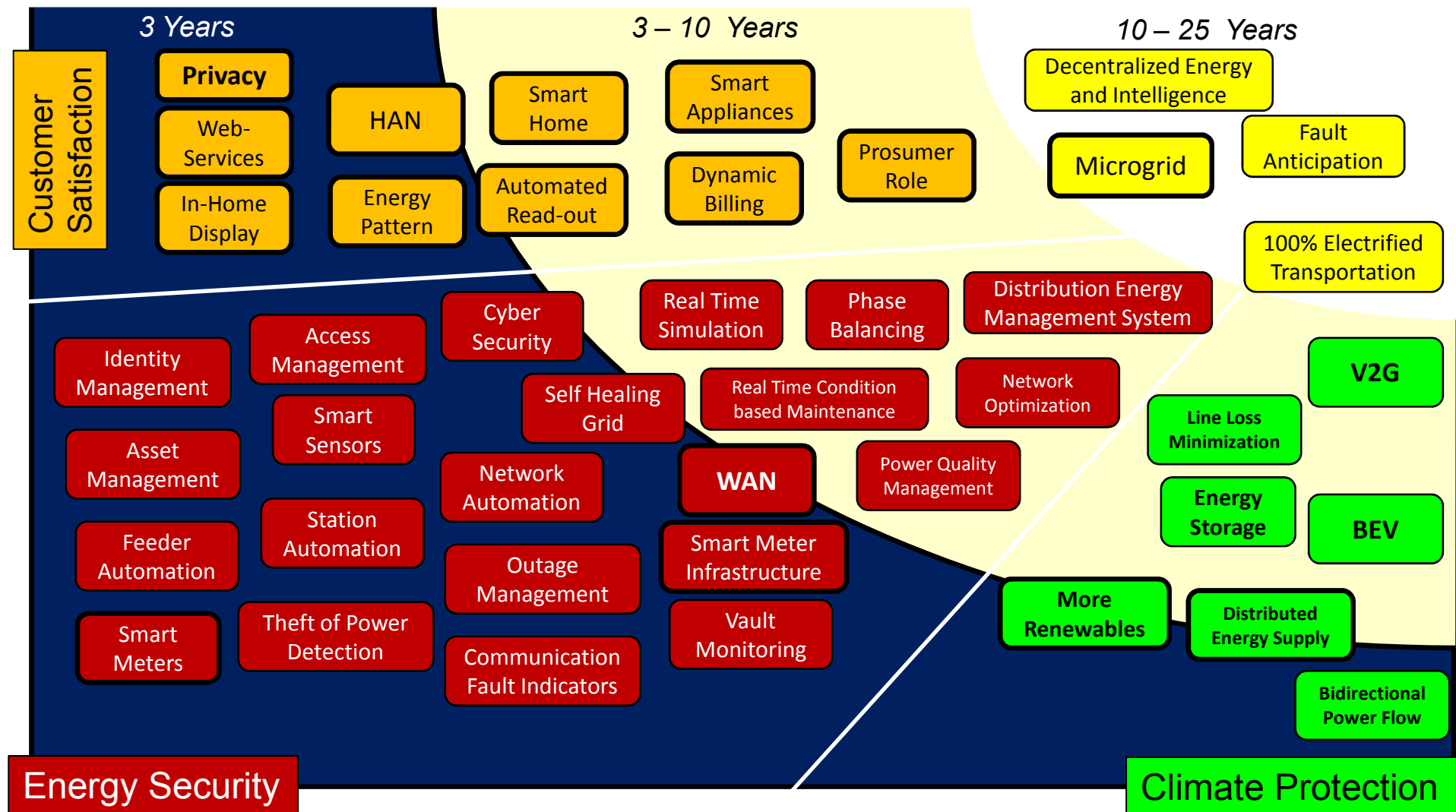
Energie - Heute

Legende:

- Höchstspannung (HH) Trafo/Umspannstation
- Hochspannung (H)
- Mittelspannung (M)
- Niederspannung (N)



Smart Grid - Vision



Probleme im Smart Energy Umfeld

Beispiele

- Privacy
- Fraud
- Cyber Crime





■ Privacy



April 2009 wurde der Gesetzesvorschlag abgelehnt, der eine verpflichtende Einführung von Smart Metern zwischen 2011 und 2016 vorsah

- Die Aufzeichnung eines 15 min Lastprofils ist nicht konform mit Artikel 8 der Europäischen Menschenrechtskonvention
- 60% der Bevölkerung sind gegen die Einführung

<http://www.wijvertrouwenslimmemetersniet.nl/>

■ Fraud

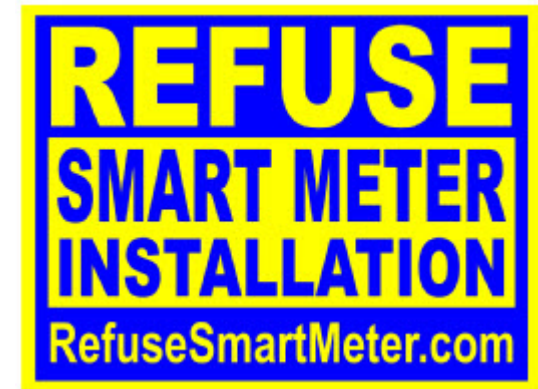
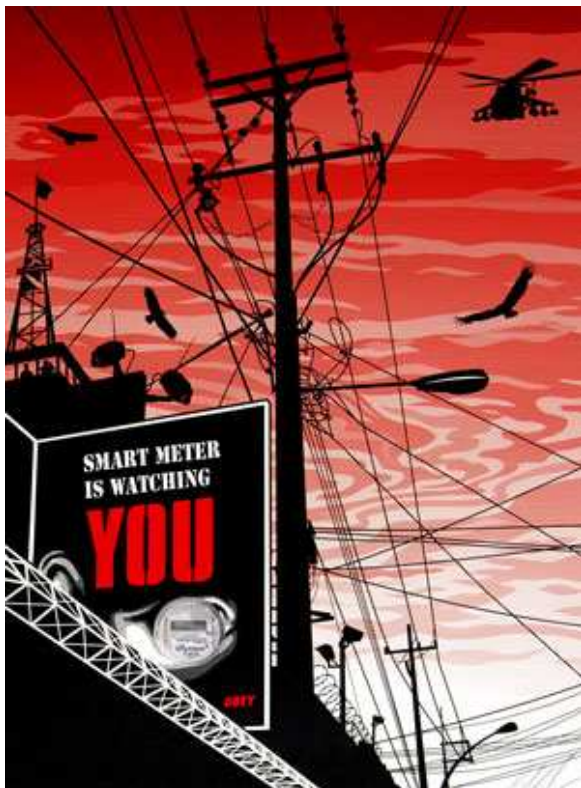


■ Cyber Cr

Probleme Datenschutz und mehr



- Privacy



<http://turn.org/>

<http://www.smartmeterfilm.com/>

<http://www.smartmeterlock.com/>

<http://stopsmartmeters.org>

<http://michiganstopsmartmeters.com/>

<http://www.citizensforsafetechnology.com/>

Probleme Datenschutz und mehr



■ Privacy

What's so smart about 'smart' meters?

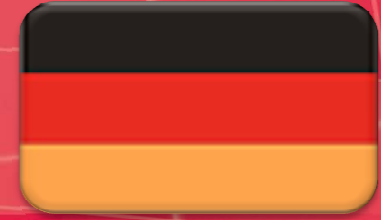


<http://www.stopsmartmetersbc.ca/html/>

<http://stopsmartmeters.com.au>

Think about smart meters. It's your life.

 www.stopsmartmeters.com.au



■ Privacy

■ Fraud

■ Cyber Crime

Smart Meter verraten Fernsehprogramm

 vorlesen /  MP3-Download

Anhand der von einem intelligenten Stromzähler gelieferten Stromverbrauchsdaten ist es möglich, auf das auf einem typischen TV-Gerät angezeigte Fernsehprogramm zu schließen, da Fernseher je nach angezeigtem Bild unterschiedlichen Strombedarf haben. Das haben [Forscher der FH Münster](#) im Rahmen des vom Bund geförderten Projekts DaPRIM (Data Privacy Management) in Versuchen [herausgefunden](#). Dabei ist es über die Auswertung des Verbrauchsmusters prinzipiell auch machbar, einen etwa von DVD oder anderen Quellen abgespielten Film zu identifizieren.

Besonders hilfreich bei dieser Analyse sind Hell-Dunkel-Abschnitte, die [besonders](#) starke [Änderungen](#) im Stromverbrauch ergeben, sowie größere Datenmengen und wenig Störungen durch andere Geräte. Bei den Versuchen griff man auf die Daten eines in einer normalen Wohnung installierten, intelligenten Stromzählers des Herstellers EasyMeter zurück, der die Verbrauchsdaten alle zwei Sekunden an einen Server eines Dienstleisters schickte. Im Kundenprofil auf dem Webserver des Anbieters ließen sich die Gesamtverbrauchsdaten des Haushalt auslesen und die Daten für den Fernseher herausrechnen und auswerten.

Bislang ging man davon aus, dass intelligente Stromzähler anhand des für bestimmte Geräte typischen Stromverbrauchs zu bestimmten Zeitpunkten nur Hinweise geben können, ob ein Kunde zum Zubereiten des Mittagessens eher die Mikrowelle, den Herd oder den Ofen benutzt. Bereits das hatte Datenschützer in den USA, in denen Smart Meter bereits weiter verbreitet sind, auf den Plan [gerufen](#). Sie forderten genaue Bestimmungen, wie Stromerzeuger mit den angefallenen Daten umzugehen haben und wie sie zu schützen sind.

Die sekundengenaue Übermittlung von Daten macht nun eine feinere Analyse möglich. Dies erfordert nach Meinung der Forscher aus Münster schärfere Datenschutzbestimmungen. Abhilfe könnte es derzeit bringen, die Zeitintervalle zu verlängern oder nur eine statistische Zusammenfassung an den Stromerzeuger oder Dienstleister zu übermitteln. Damit würden keine hochaufgelösten Verbrauchsdaten für eine feinere Analyse mehr anfallen. In beiden Fällen ist der Kunde jedoch auf Maßnahmen seines Anbieters angewiesen.

<http://www.heise.de/security/meldung/Smart-Meter-verraten-Fernsehprogramm-1346166.html>
<http://www.daprim.de>

Probleme Betrug



■ Privacy

September 2010: Criminals across the **UK** have hacked the new key card system used to pop up pre-payment energy meters and are going door-to-door, dressed as power company workers, selling illegal credit at knock-down prices

The pre-paid power meters use a key system. Normally people visit a shop to put credit on their key, which they then take home and slot into their meter.

■ Fraud

FBI Concerned About Smart Meter Hacking (April 9, 2012)

According to an FBI cyber bulletin, an unnamed utility company in **Puerto Rico** was the target of attacks against smart meters, costing the company hundreds of millions of dollars. This appears to be the first report of such attacks and the FBI expects that the occurrence of similar attacks will rise as the smart grid technology is more widely adopted. The FBI believes that former employees of the meter manufacturer reprogrammed meters for between US \$300 and US \$3,000 so that the associated buildings appeared to be consuming less power than they actually used.

Most meters are read remotely, making fraud detection difficult. The alterations require physical access.

■ Cyber Crime

Probleme Cyber Crime

Gefahr für Industrieanlagen aus dem Netz

Mindestens 10.000 Steuerungssysteme (SCADA), unter anderem von Kraftwerken und Energieversorgern, sind im Internet sichtbar, viele davon sogar mit Log-in-Formular. Sie sind damit leicht angreifbar.

Montagmittag hatte @HEX0010 auf Twitter noch bekanntgegeben, dass es auf dem Sozialen Netzwerk Pastebin Interessantes zum Thema "SCADA" zu sehen gebe. Auf Pastebin fand sich die Nachricht, dass zwei der Steuerungsanlagen für Industriesysteme (Supervisory Control and Data Acquisition, SCADA) erfolgreich angegriffen und gehackt worden waren. Auf YouTube wurde ein kleines Video veröffentlicht, das die grafische Oberfläche eines solchen SCADA-Systems zeigt.

Nach einem weiteren Tweet merkte ein anderer Benutzer an, dass wohl am Interessantesten an diesen beiden Postings sei, dass nun bereits SCADA-"Exploits" über Twitter zum Kauf angeboten würden. Exploits sind kleine Programme oder Skripts, die eine Sicherheitslücke ausnützen und so einen Angriff ermöglichen. Wenig später war das Twitter-Konto von @HEX00010 bereits gelöscht.

31. 1. 2012 - 16:00

29. 2010

Smart Products | Smart Meters Vulnerable to Hack Attacks

By David Sims
Contributing Editor

Now smart meters designed to help deliver electricity more efficiently are inviting – and vulnerable – targets for hackers, security analysts say. The Associated Press (News - Alert) reports that hackers can access the power grid "in previously impossible ways" from hacking the meters.

Smart Meter Worm Could Spread Like A Virus

By Katie Fehrenbacher | Jul. 31, 2009, 7:35am PDT | 2 Comments

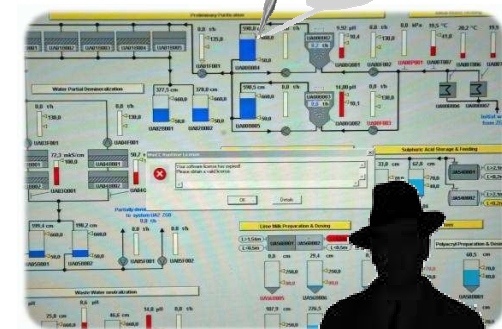
Tweet

Gefällt mir

Registrieren, um sehen zu können, was deinen Freunden gefällt.

For a utility that's in the process of installing smart meters, there are probably few things more terrifying than the simulation of a smart meter worm that IOActive's Mike Davis showed off at the annual security conference Black Hat on Thursday. During Davis' presentation, he showed how he and his team at the security consulting

Stuxnet



Source: <http://www.freitag.de/community/blogs/sachichma/stuxnet-der-suesse-hack>

■ Cyber Crime

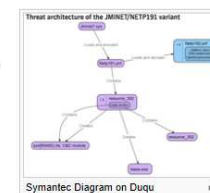
Duqu

From Wikipedia, the free encyclopedia

Duqu is a computer worm discovered on 1 September 2011, thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS)^[1] of the Budapest University of Technology and Economics in Hungary, which discovered the threat, analyzed the malware and wrote a 60-page report^[2], naming the threat Duqu.^[3] Duqu got its name from the prefix "DQ" it gives to the names of files it creates.^[4]

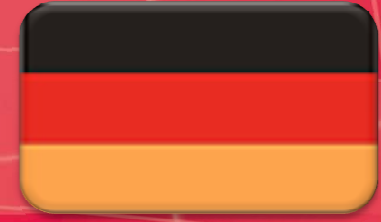
Contents [hide]

- The Duqu term
- Relationship to Stuxnet
- Microsoft Word zero-day exploit
- Purpose
- Additional Resources
- See also
- References



Aktivitäten im Energiesektor

IT Security für Smart Meter



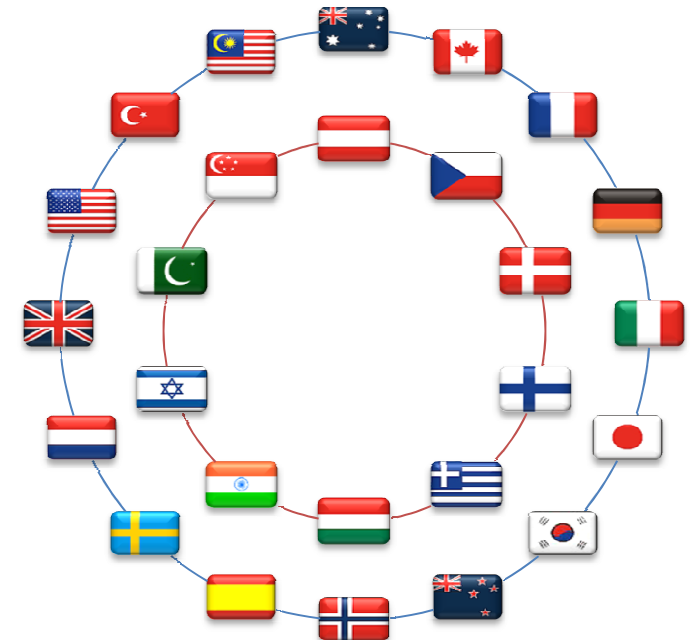
IT Security Funktionalitäten

wurden für **Smart Meter Systeme** vom **BSI**
(mit **TÜViT**) spezifiziert - zusammen mit:

- BMWi
- BNetzA
- PTB
- BfDI
- *Schutzprofile (Protection Profiles)* nach den internationalen



https://www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter_node.html



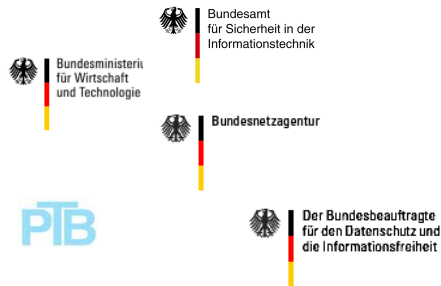
Gesetzgebung

- **EU Direktive:** Roll out von Smart Meter Geräten
- **EnWG** im Sommer 2011
 - Gateway erforderlich für eine große Anzahl Konsumenten
 - Neue Installationen
 - Nutzer > 6000 kWh
 - Prosumer (z.B. bei Solaranlagen), falls > 7 kW
 - Ausschließlich zertifizierte Geräte dürfen installiert werden
 - Übergangszeitraum
- Gültig ab **2013**

Nationale Entwicklung



- BSI
- BMWi
- BNetzA
- PTB
- BfDI

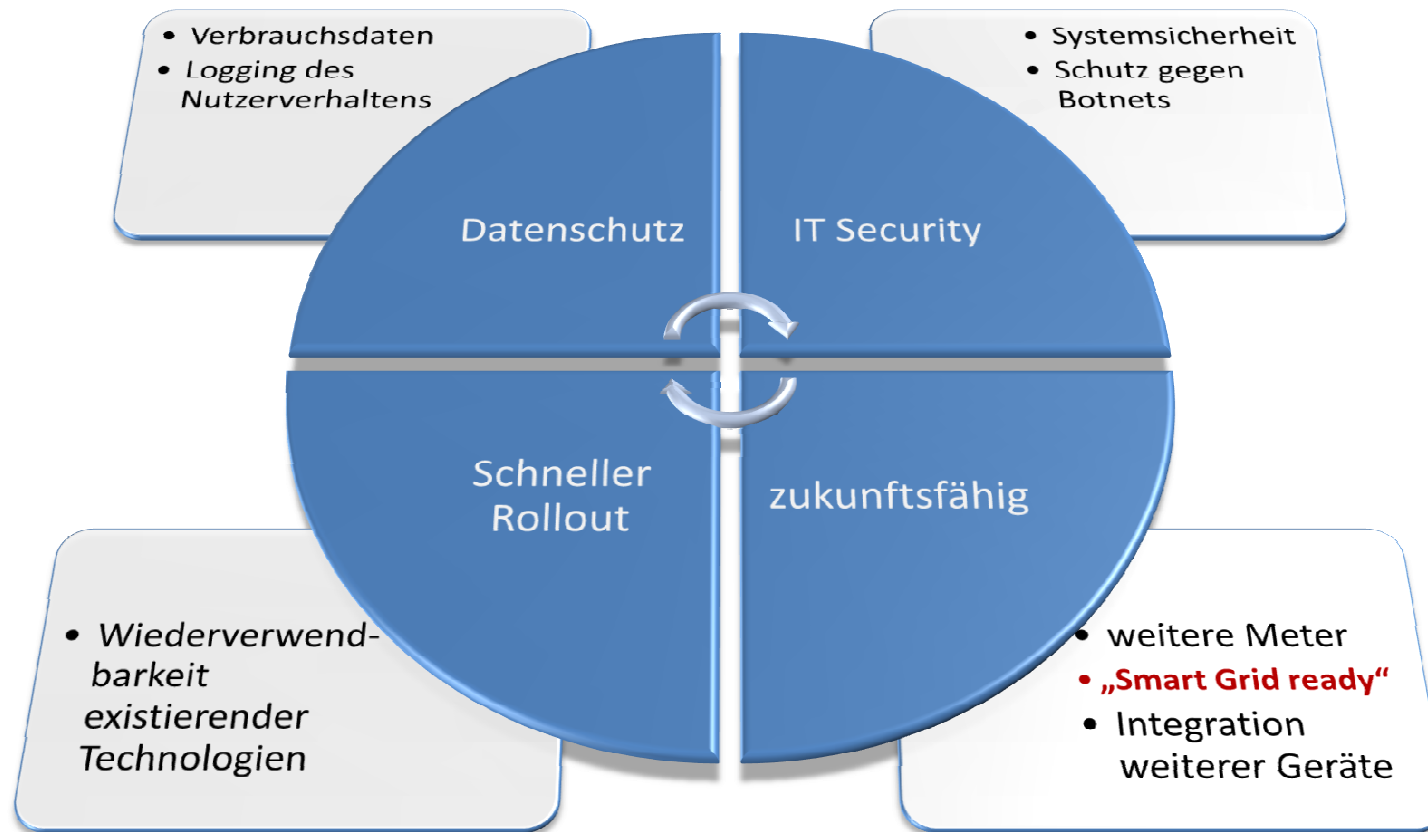


Teilnahme von mehr als 20 Verbänden

- Kommentierungsrunden mit Podiumsdiskussionen
- > 2000 Kommentare



Die technische Herausforderung

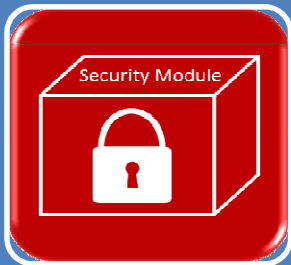


Der System Ansatz



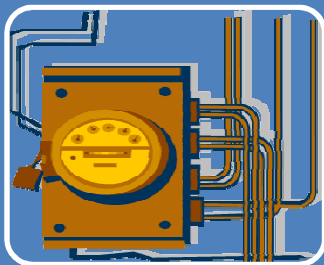
Gateway

- Zentrale Komponente eines Smart Meter Systems
- Vielfalt an Funktionalität
- Hohe Prüftiefe



Security Module

- Implementierung von Kryptographie
- Sichere Schlüsselmanagement
- Unterstützung eines schnellen Rollouts durch Wiederverwendung von existierenden Technologien



Smart Meter System

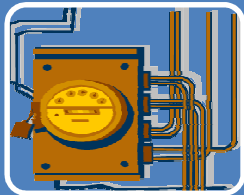
- Umfasst Gateway und mehrere Meter

Hauptfunktionalität des Gateway



Firewalling

- Gateway besitzt Informationsflusskontrolle
- Verbindungsaufbau geschieht immer vom Gateway
- Das Gateway lässt keinen Verbindungsaufbau von extern zu



Meter Policies

- Das Gateway bekommt Daten von den Metern
- Das Gateway verarbeitet Daten zu installierten Profilen
- Das Gateway versendet die verarbeiteten Daten zu externen Backends im WAN



Datenschutz

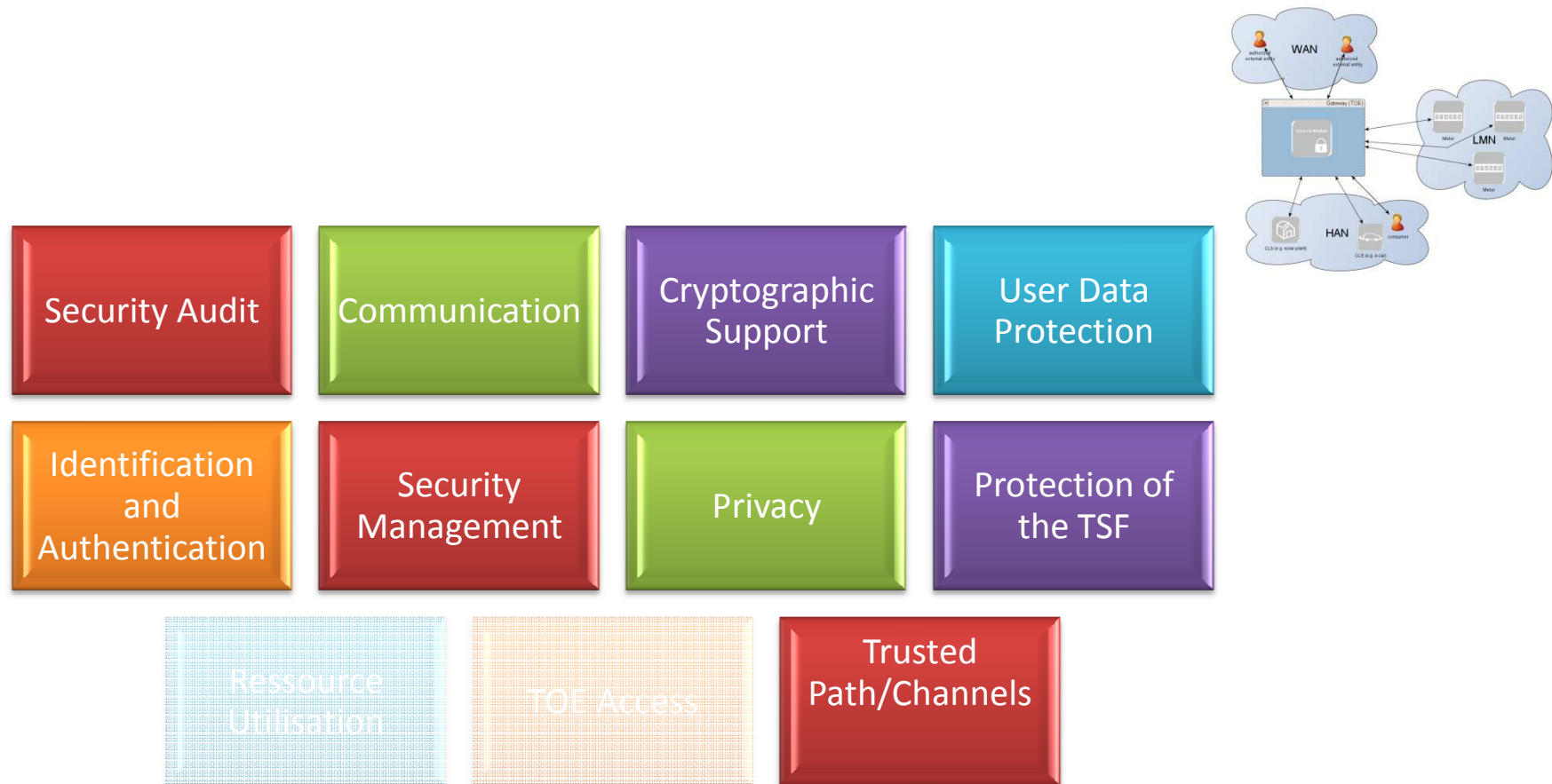
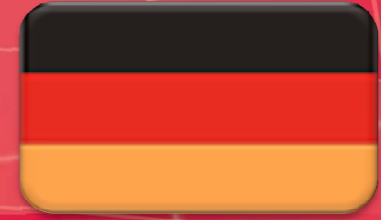
- Der Informationsfluss ist transparent für den Endverbraucher
- Das Gateway erlaubt nur verschlüsselten und authentischen Informationsfluss
- Das Gateway kann den Informationsfluss verschleiern, falls notwendig



Kommunikation für CLS

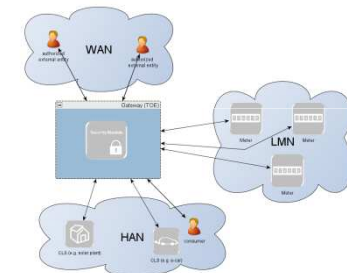
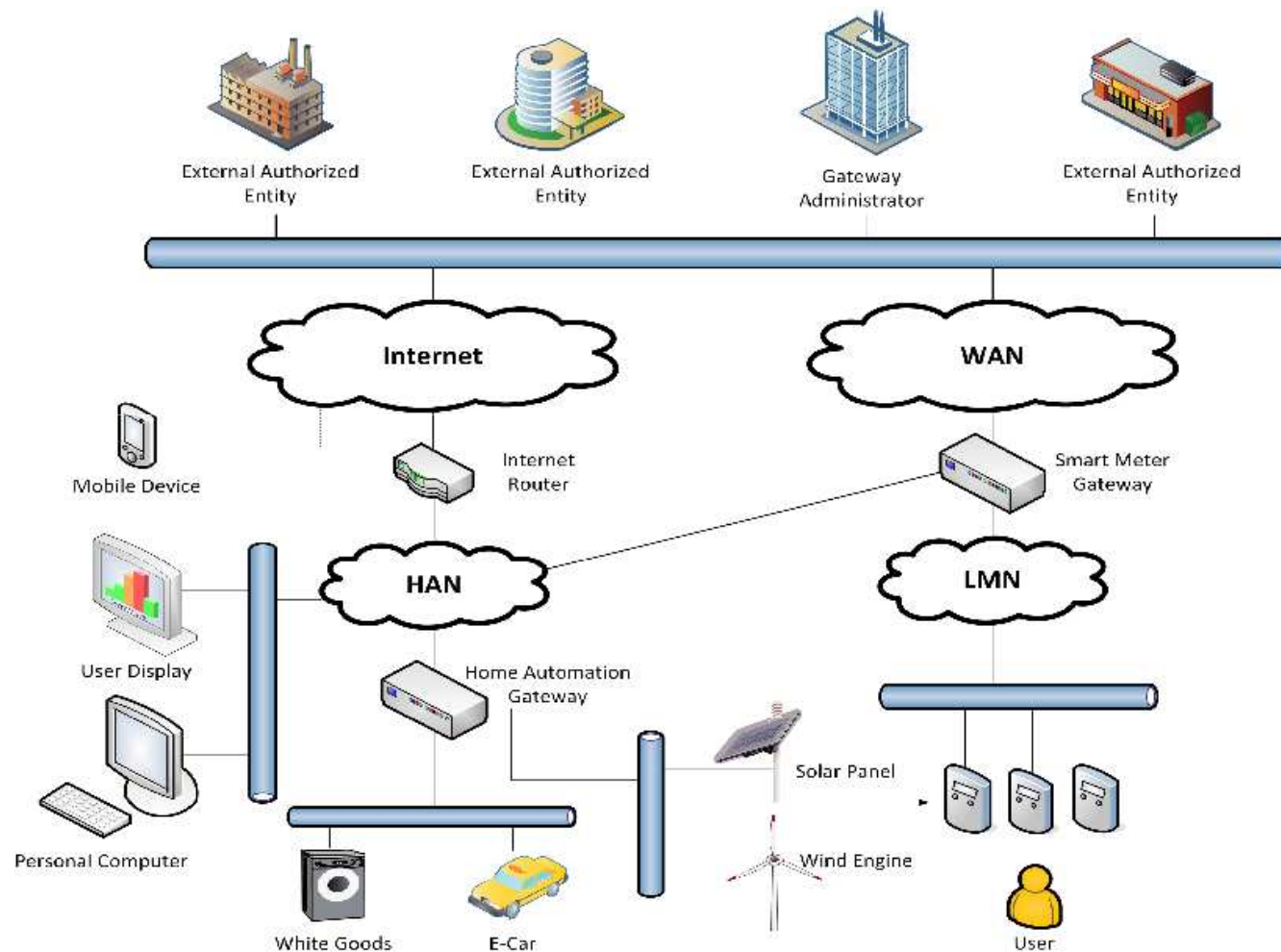
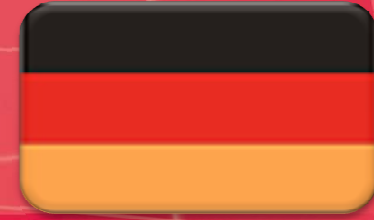
- Das Gateway erlaubt „Controllable Local Systems“ mit Backendsystemen im WAN zu kommunizieren
- Die CLS müssen die Policies des Gateways für den Informationsfluss erfüllen

Security Features Smart Meter Gateway



IT Security für Smart Meter

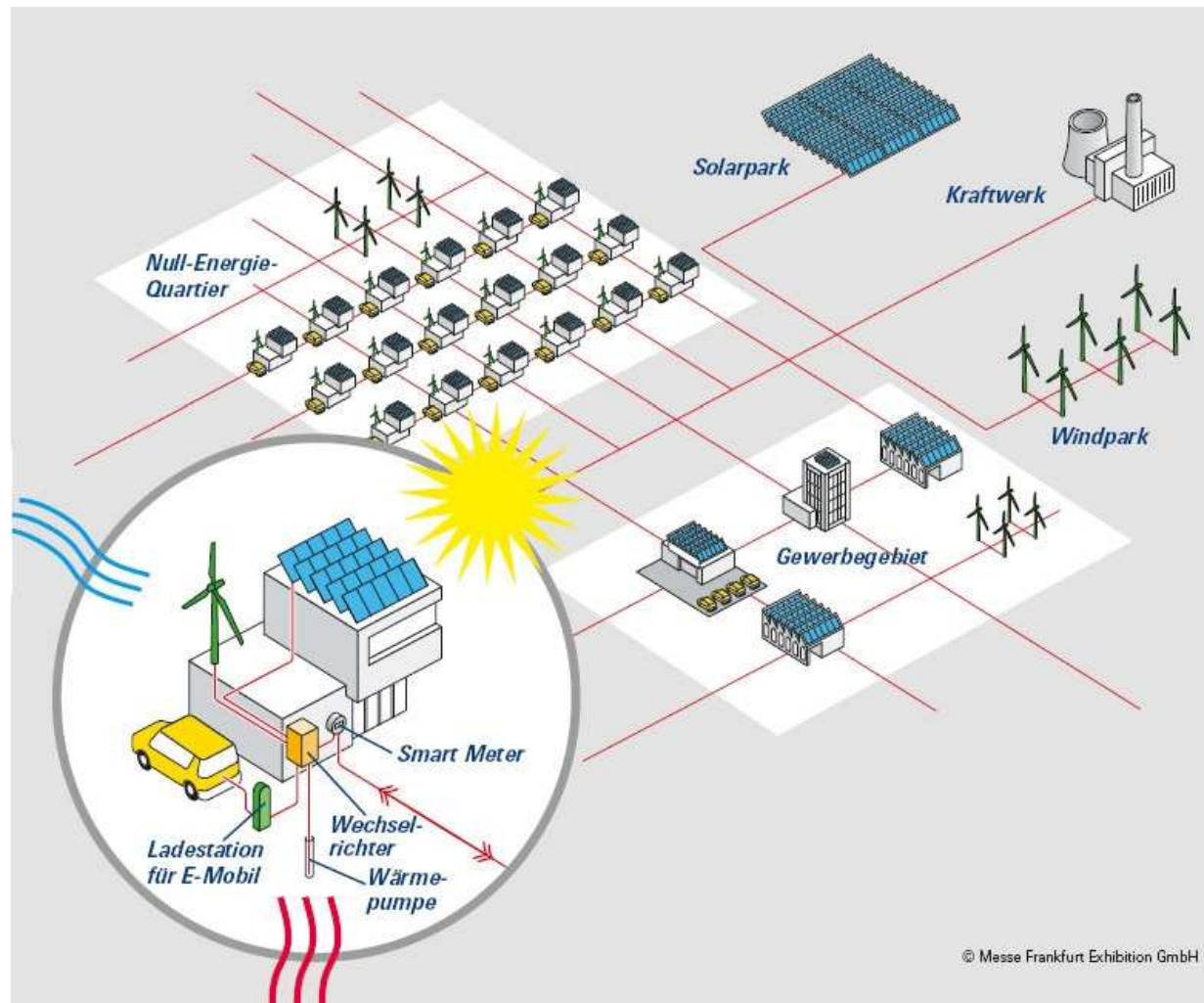
Gesamtsystem → BSI TR-03109



1. **PKI**
2. **Kryptographie**
3. **Security Module**
4. **Kommunikation**

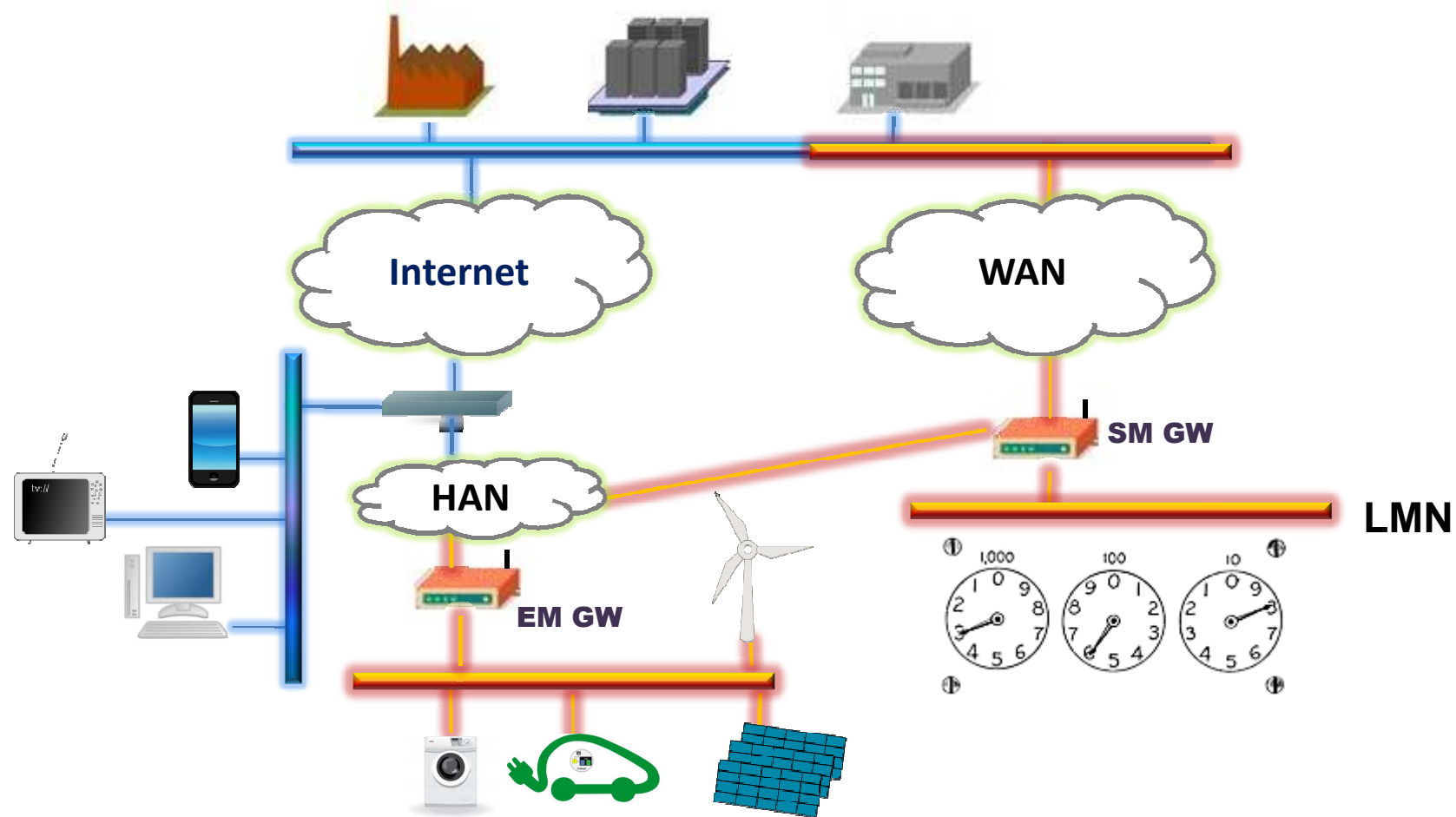
Light & Building

Gebäude als Kraftwerk im Smart Grid



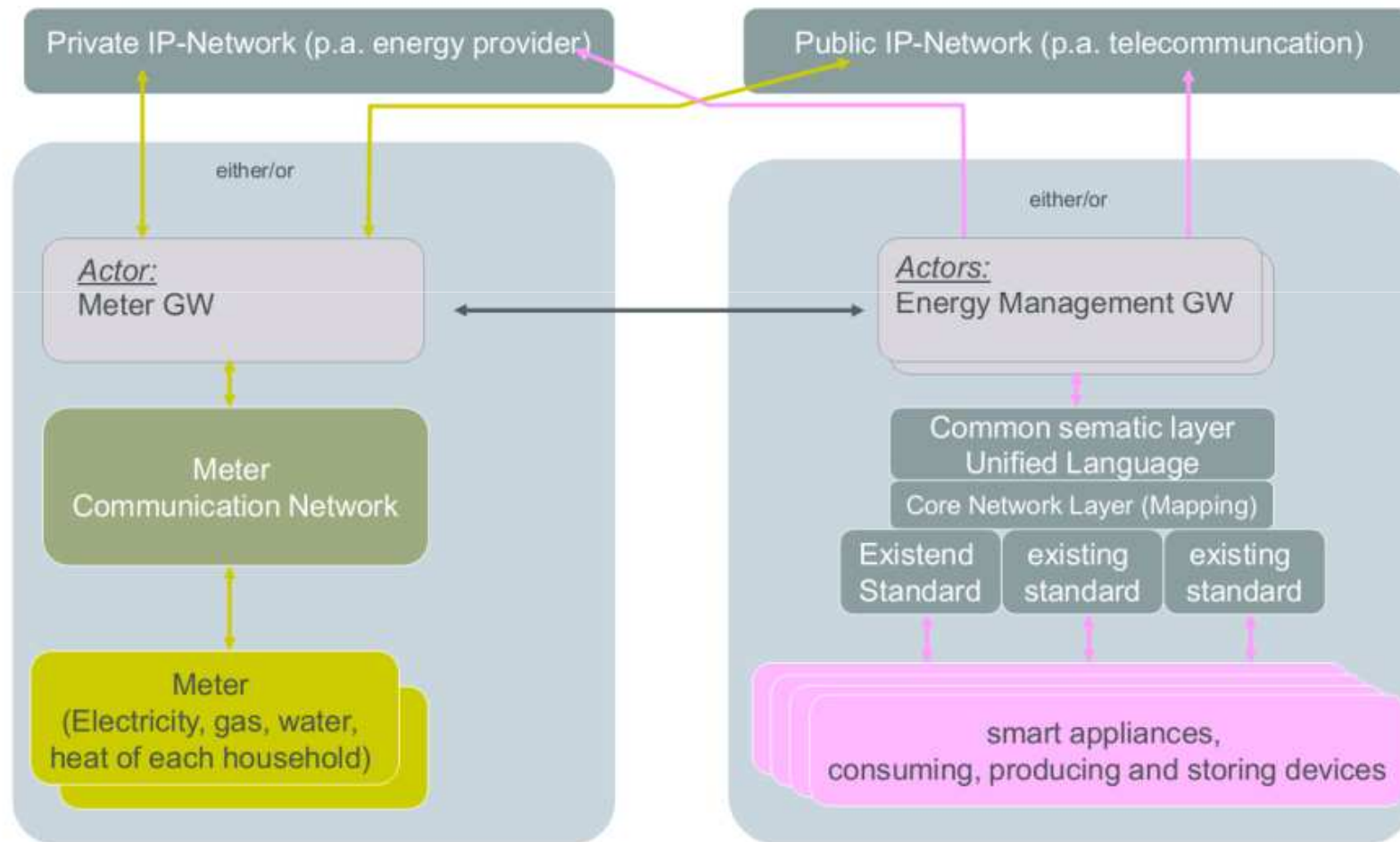
Architektur (1)

Diskussionsgrundlage

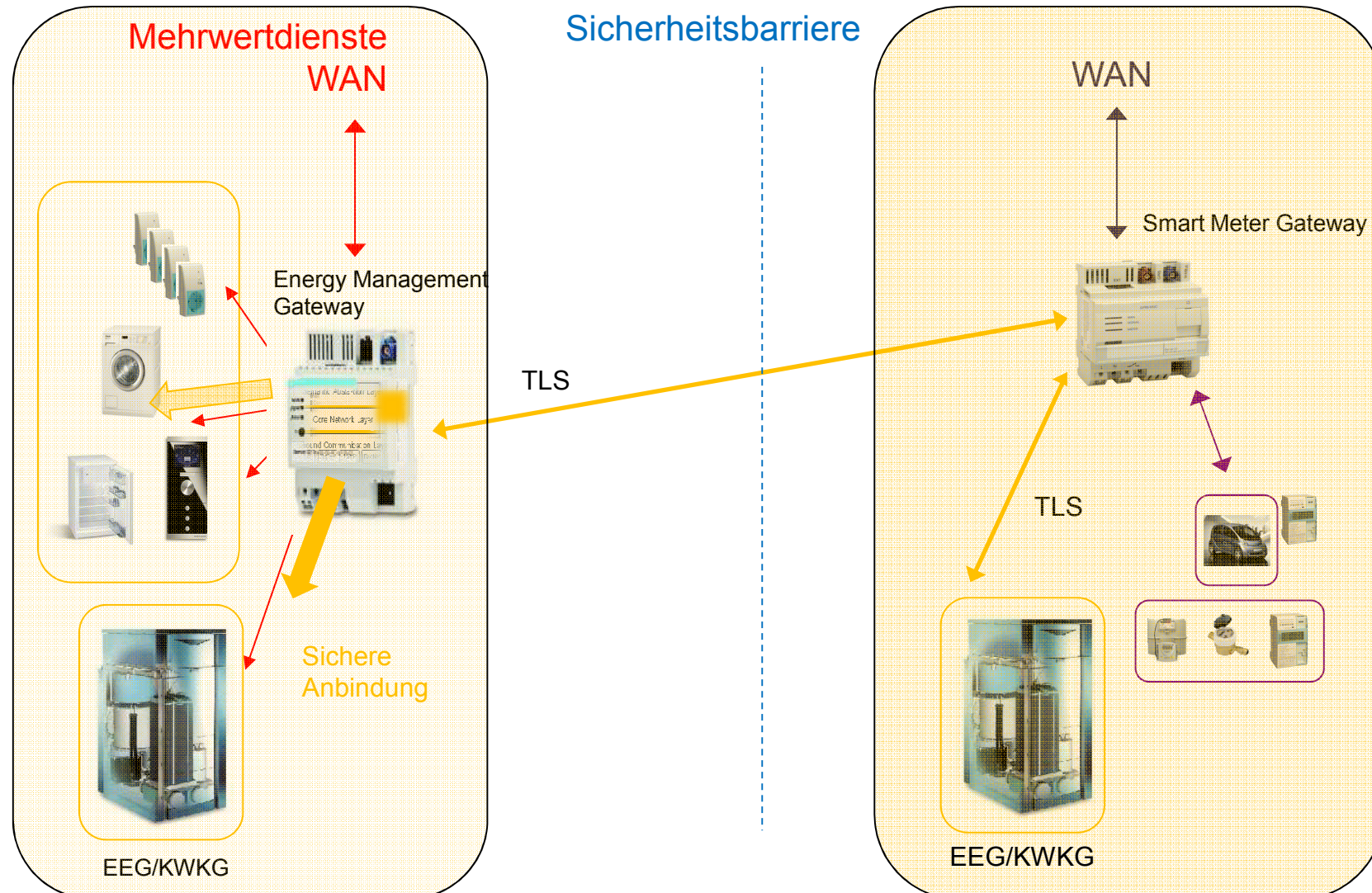


Energiemanagement

Generelle Architektur aus CEN/Cenelec/ETSI



Energiemanagement Aufgabenstellung - Idee



DKE 716

Normative Beschreibung eines Sicherheitskonzeptes für Energiemanagement

DKE Deutsche Kommission
Elektrotechnik Elektronik Informationstechnik
im DIN und VDE



Deutsches Mitglied in IEC und CENELEC

Beschlussvorlage für STD 1911 „Lenkungsreis Normung E-Energy / Smart Grids“

Titel: Referenzarchitektur: funktionale Trennung von Energiemanagement und Smart Meter Gateway im Kontext des BSI- Schutzprofils für Smart Meter Gateways

Basis:
Eckpunktepapier
DKE & BSI ; 11.11.2011

Beschlussvorlage
STD 1911 „Lenkungsreis Normung
E-Energy / Smart Grids“ ; Januar 2012

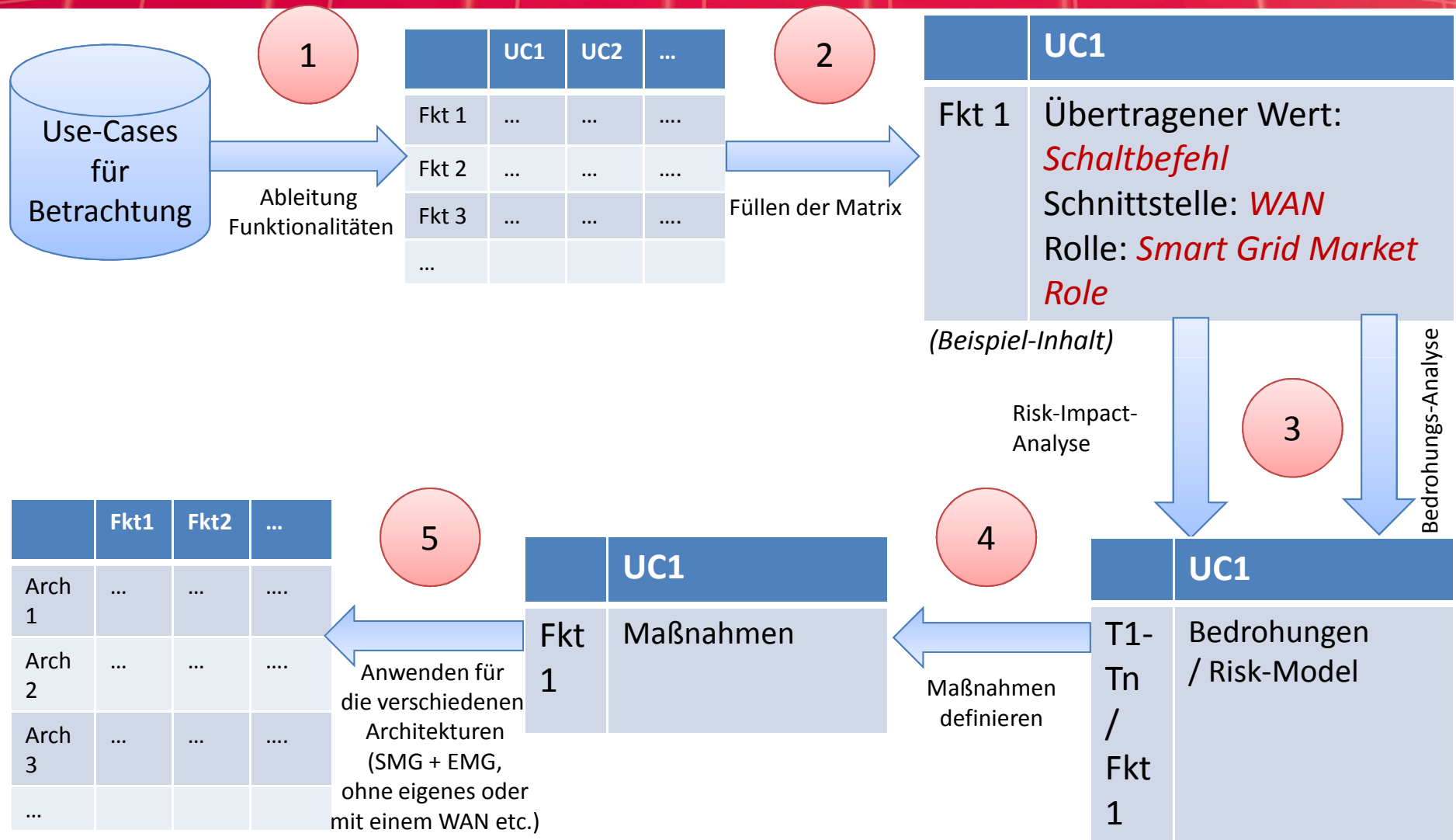
Erstellung der

- **normativen Beschreibung** eines **Energiemanagementgateways**
 - im Konsens mit dem *BSI* und
 - im Kontext der *internationalen Normung*
- so durchzuführen, dass bei den gesetzlichen Regularien (insbesondere beim EnGW) in Zukunft das Energiemanagement eigenständig *oder* ergänzend zu der Domäne *Smart Metering System* eingesetzt werden kann.

Dabei ist zu berücksichtigen, dass das Gateway auch für andere (Mehrwert-) Dienste eingesetzt werden kann bzw. als Bestandteil übergreifender (z.B. Smart Home / Building) Systeme realisiert werden kann.

DKE 716

Vorgehensweise



DKE 716

Stand der Use-Cases

Nr	Name
1	AK716.0.1_UC1_Direct control for (object) devices according to EnWG §14a
2	AK716.0.1_UC2_Provision of an incentive value for a connection object
3	AK716.0.1_UC3_Direct control for (object) devices according to EEG §6
4	AK716.0.1_UC4_Operation Demand Side Management
5	AK716.0.1_UC5_Visibility of Energy Management Data
6	AK716.0.1_UC6_Data tunneling and remote administration of (Object) devices
7	AK716.0.1_UC7_EMG_OD_Registration
8	AK716.0.1_UC8_Administration EMG



EU Mandat M/490:
Use Cases auf
europäischer Ebene

Frankfurt,
26. Januar 2012

Johannes Stein
VDE/DKE,
Vorsitzender der
Arbeitsgruppe "Sustainable Processes"
Smart Grid Coordination Group (SG-CG)
CEN / CENELEC / ETSI

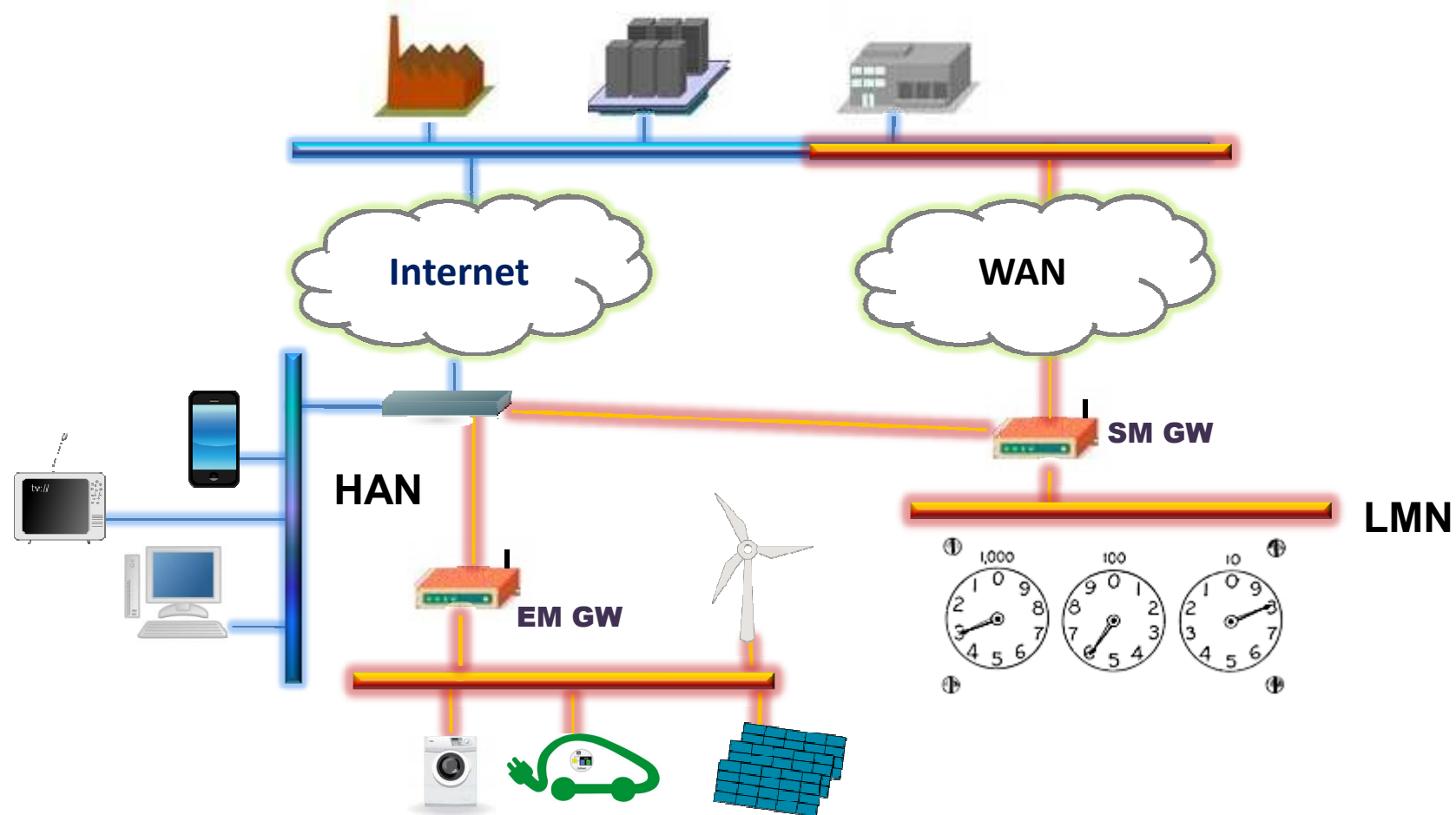
weitere Use-Cases:

Generic Use-Cases aus M490, soweit verfügbar

*M490 betrachtet nur Smart Grid relevante Use-Cases,
keine rein Home Automation relevanten Use-Cases*

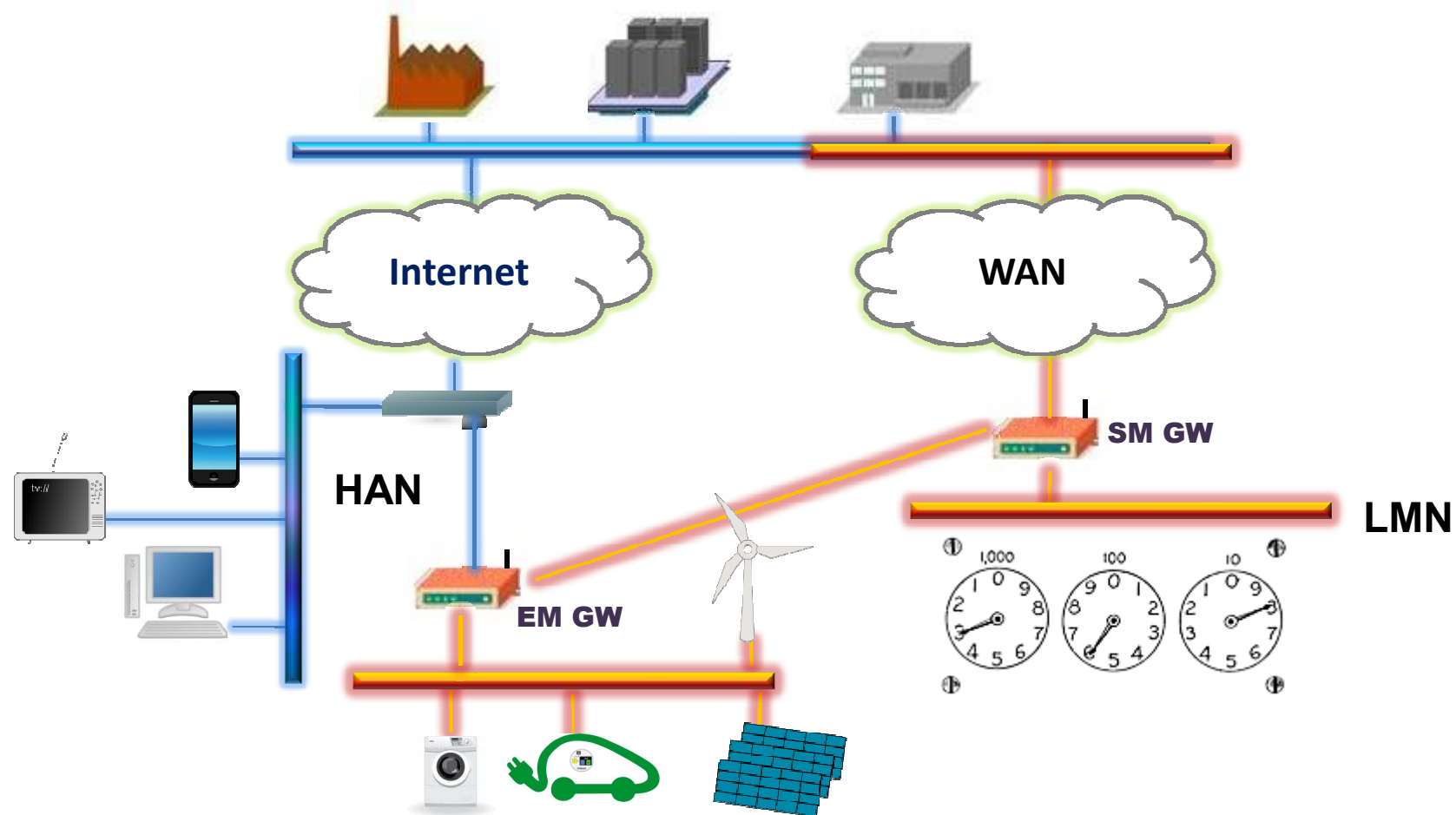
Architektur (2)

Synergie EM-SM



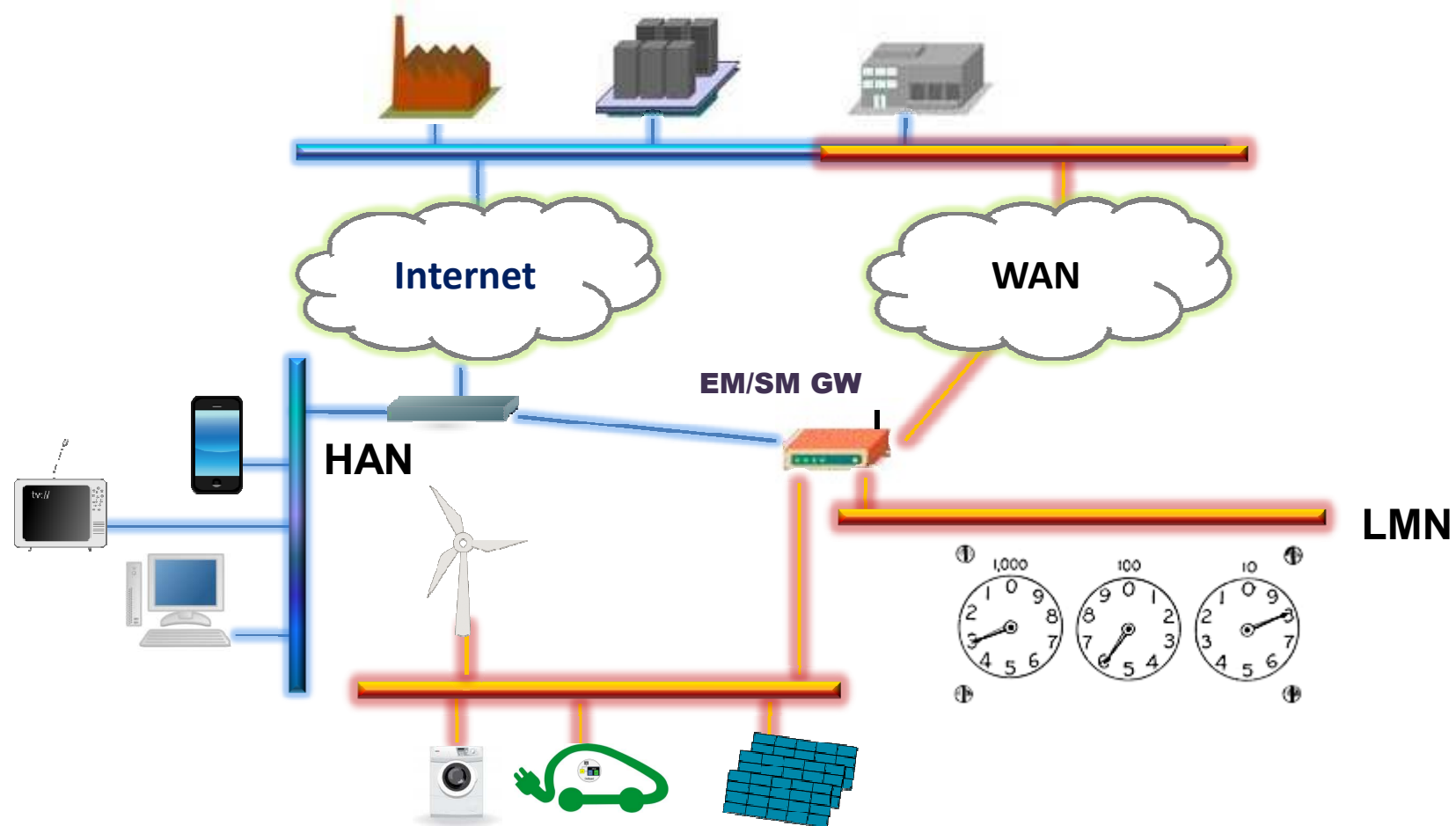
Architektur (3)

Synergie EM-SM



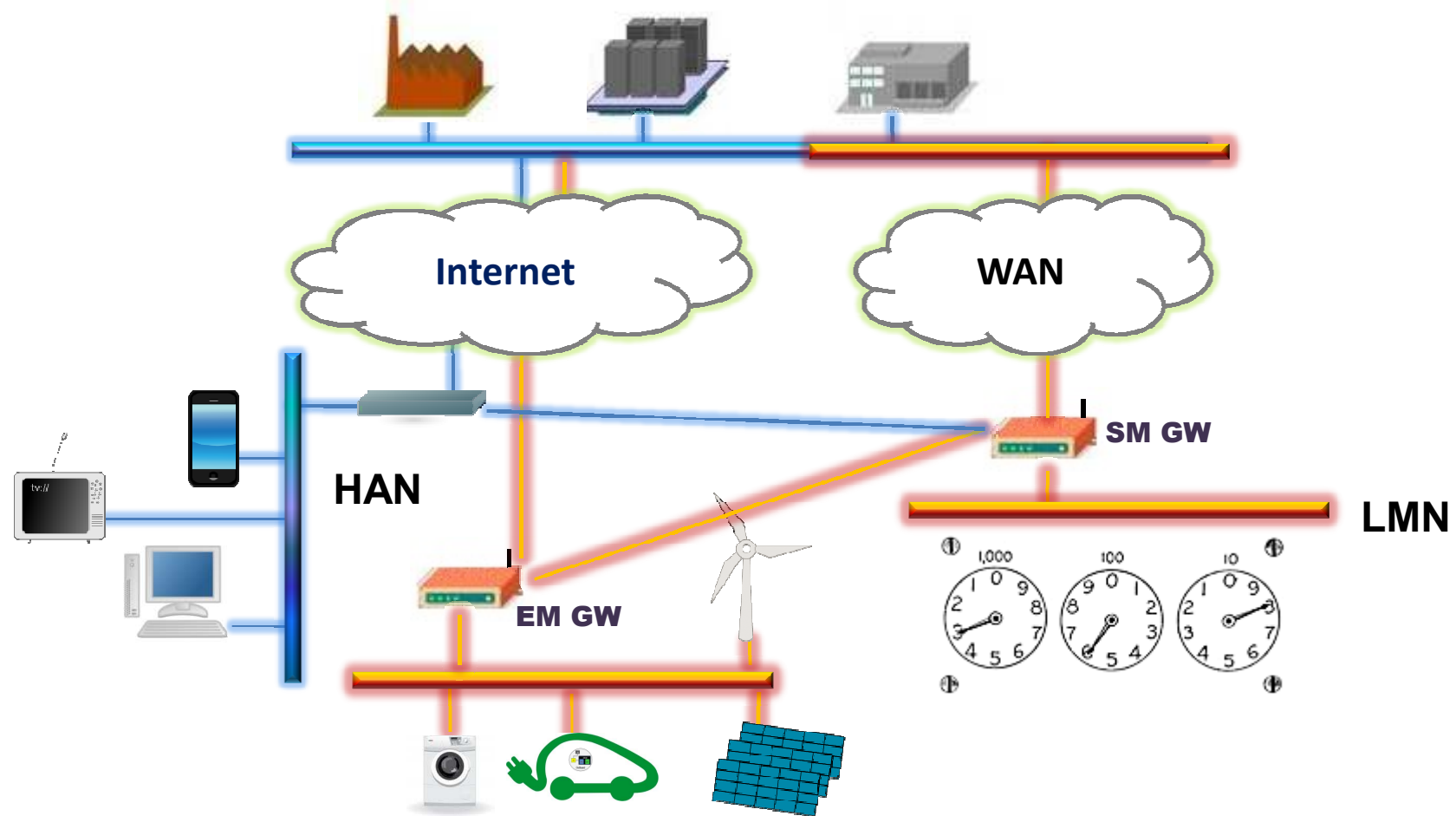
Architektur (4)

Kombination EM-SM



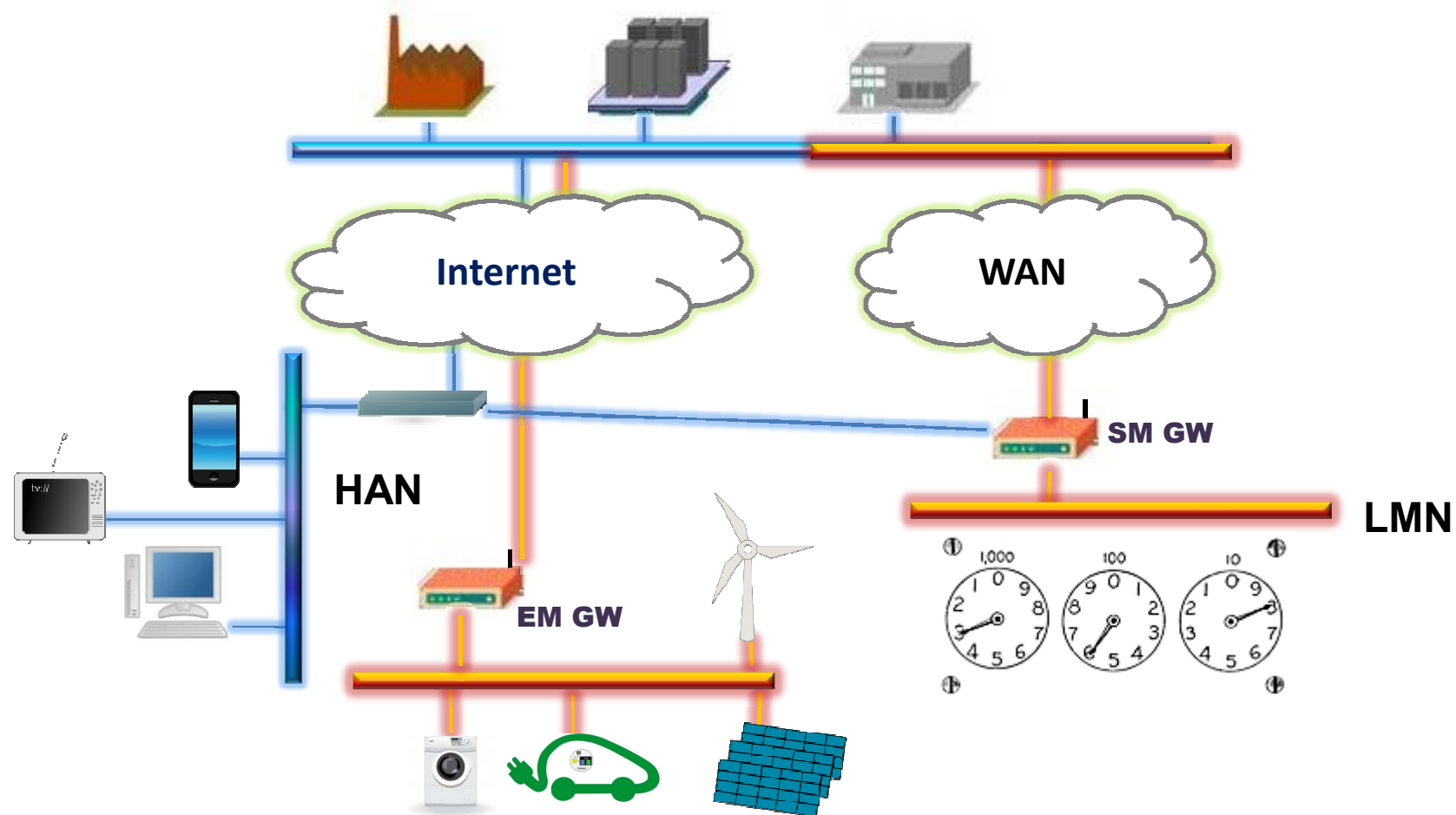
Architektur (5)

Separierung EM-GW



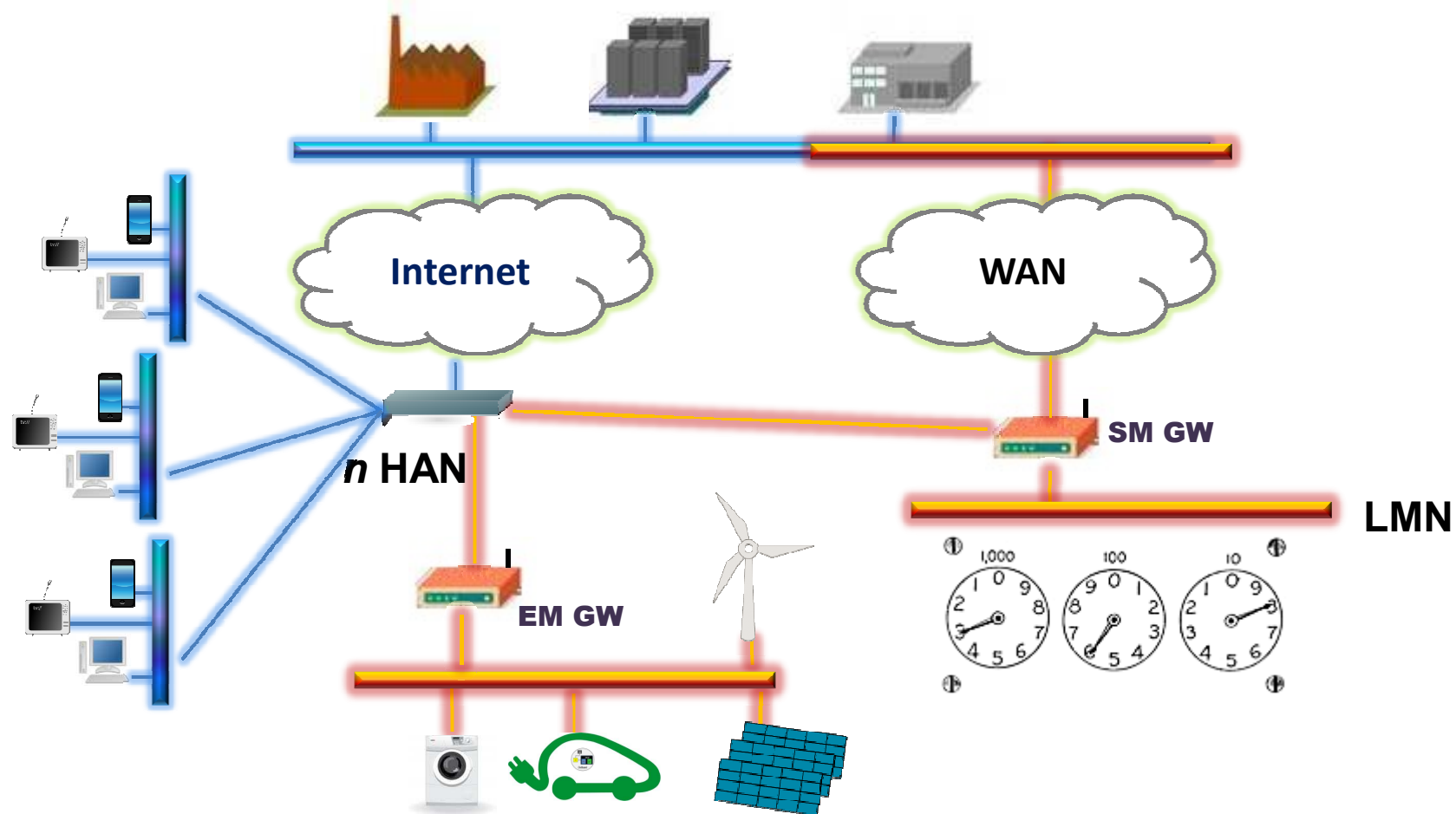
Architektur (6)

Entkopplung EM-GW



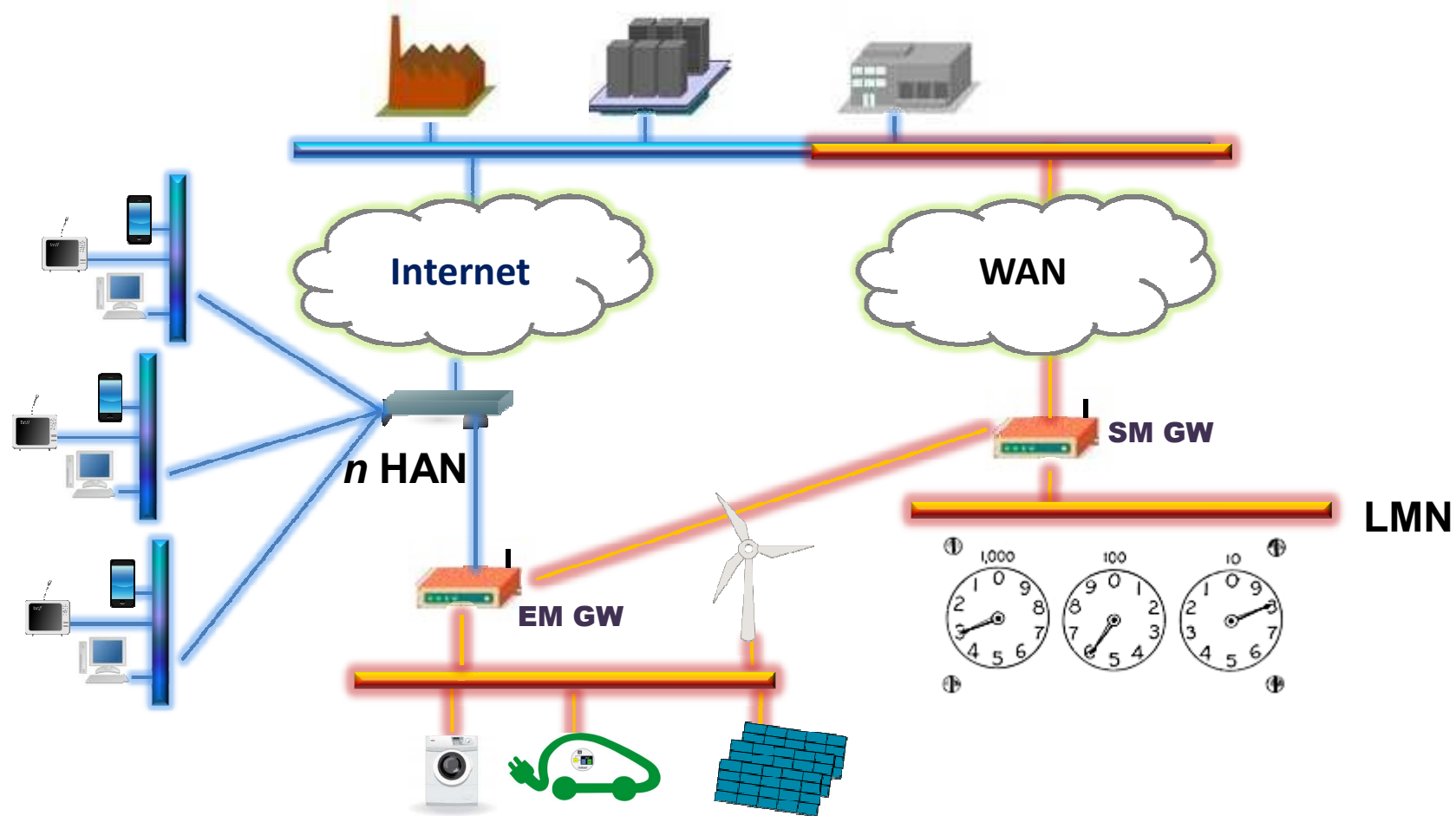
Architektur (7)

Mandantenfähigkeit - Synergie EM/SM



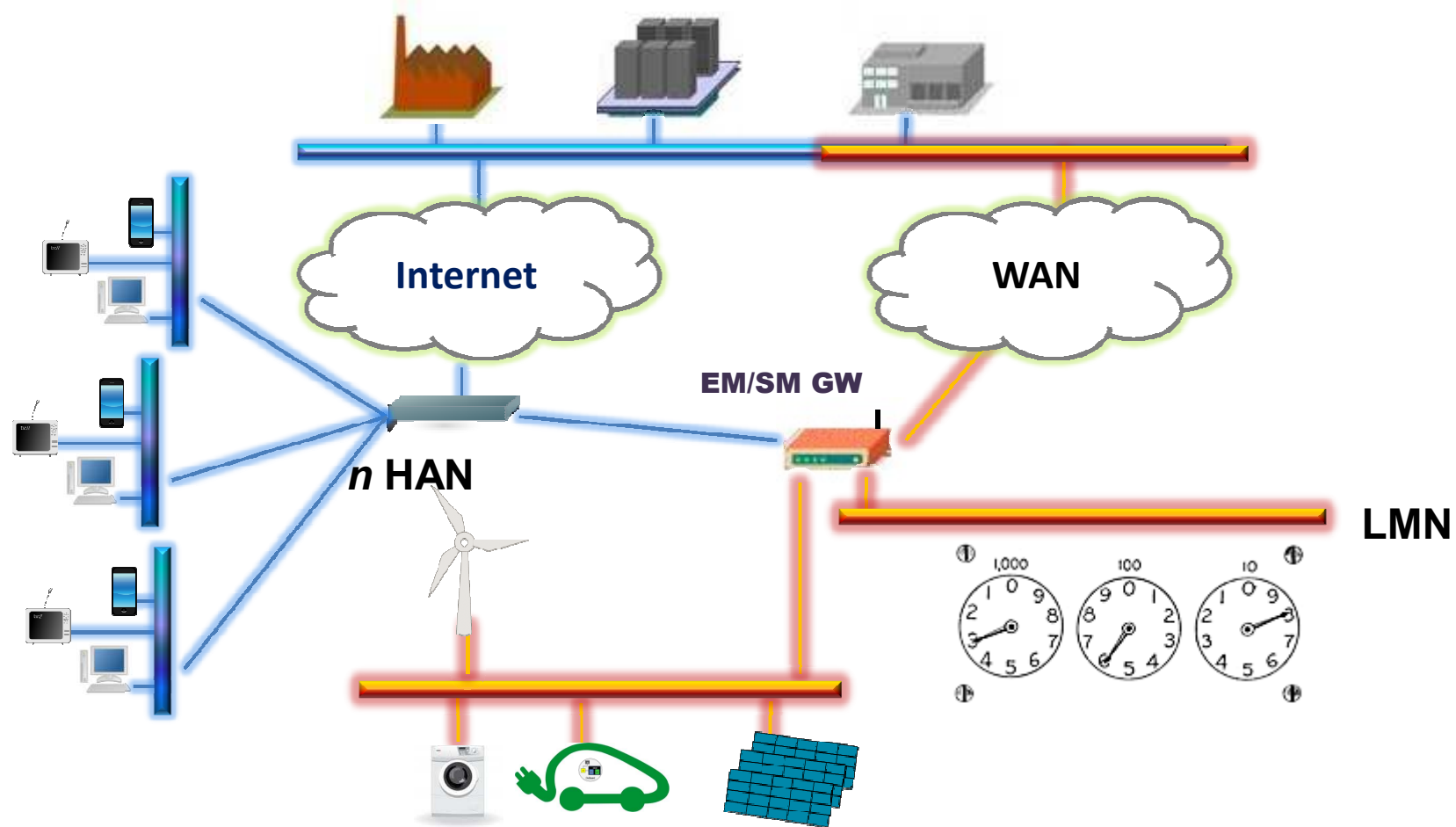
Architektur (8)

Mandantenfähigkeit - Synergie EM-SM



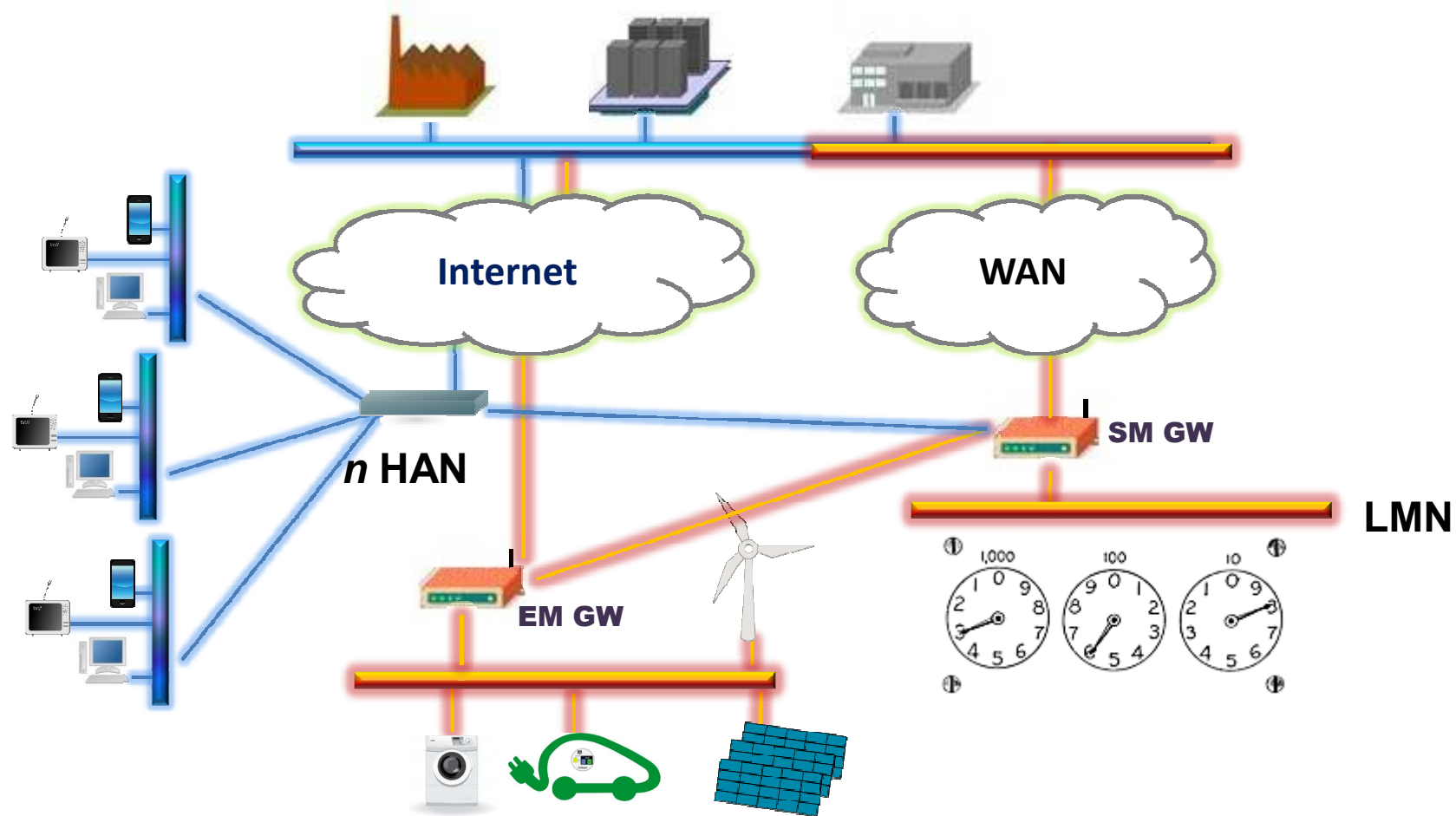
Architektur (9)

Mandantenfähigkeit - Kombination EM-SM



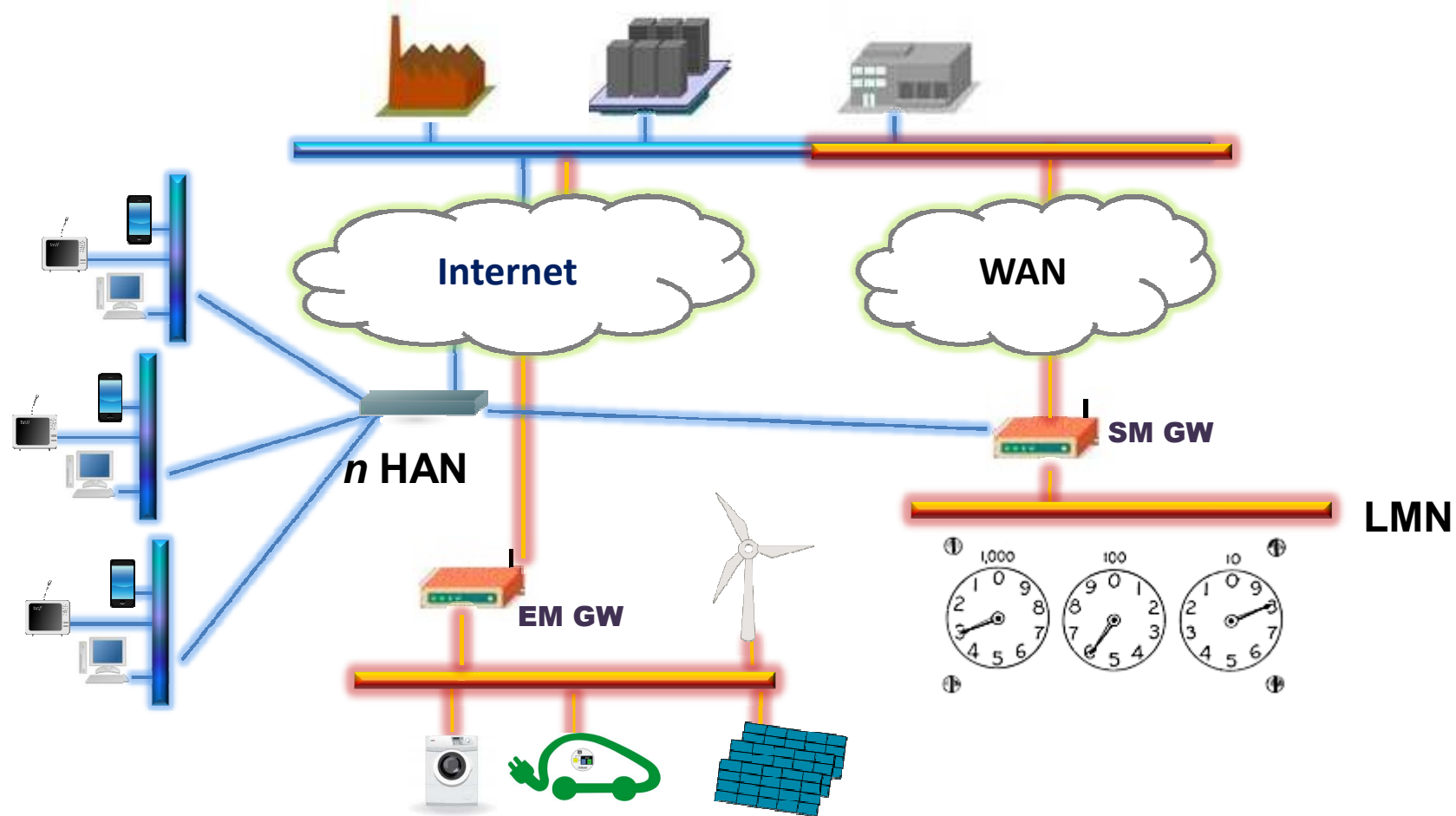
Architektur (10)

Mandantenfähigkeit - Separierung EM-GW

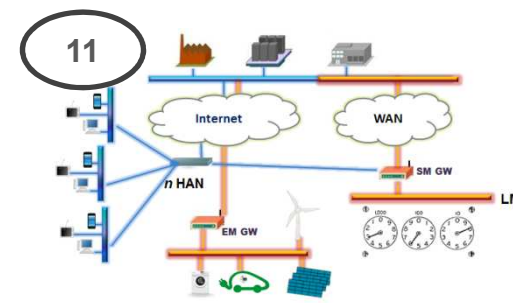
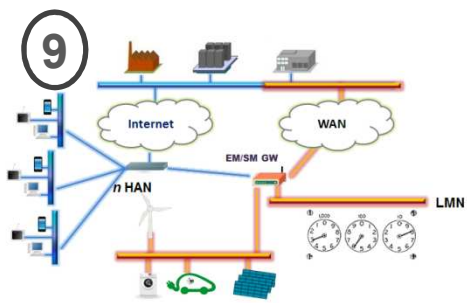
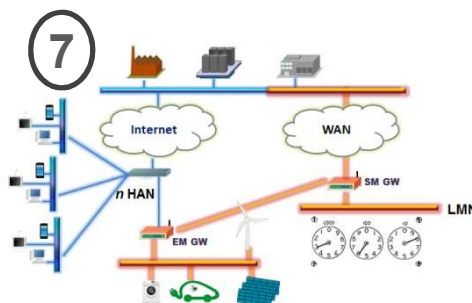
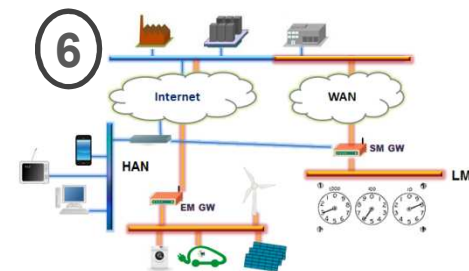
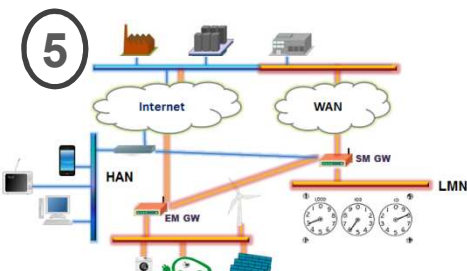
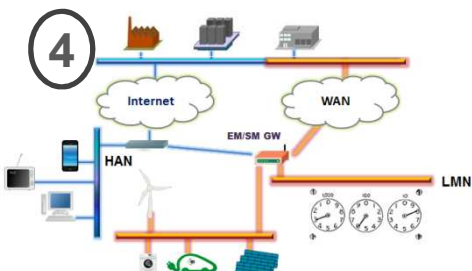
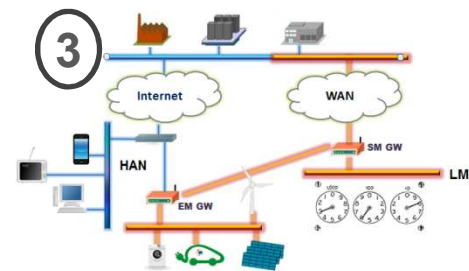
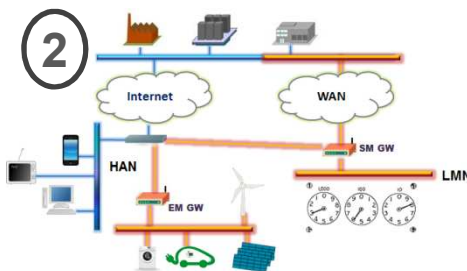
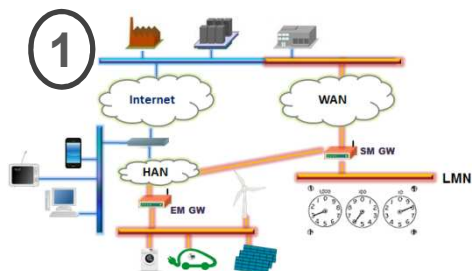


Architektur (11)

Mandantenfähigkeit - Entkopplung EM-GW



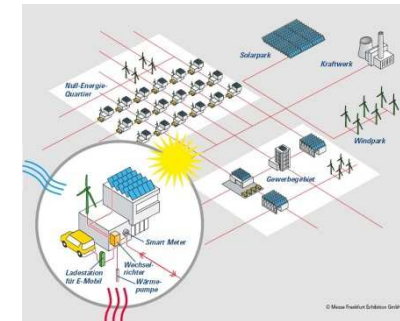
Architekturen



Smart Home

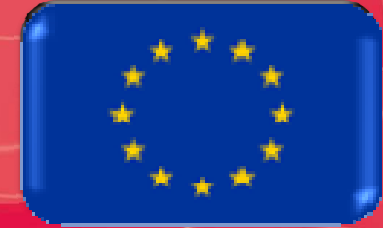
weitere Themen zu: IT Security / Datenschutz

- Telefonie / Internet
- Metering / Submetering
- Energiemanagement
- eMobility
- Klima / Heizung
- TV / Entertainment
- Licht / Beschattung
- Alarm
- Zutritt



→ Synergien !

Europa: „Privacy by Design“



1. Datenschutz - im Sinne des Endverbrauchers - ist **wichtiger Bestandteil** von Smart Meter Systemen
2. Zentrale Funktionalitäten im Smart Meter Systems unterstützen den Datenschutz (**Design Feature**)
3. Datenschutz „**by default**“
4. Datenschutz ist **transparent** für den Endverbraucher
5. Durchgängiger Datenschutz im **Life-Cycle** des Gesamtsystems

Empfehlung der EU Kommission (09.03.12)

Vorbereitung für die Einführung intelligenter Messsysteme

„Gründe“ - Auswahl



- **EU Direktive**
- **Artikel 8** der Charta der Grundrechte der EU
- **Einbau** von Datenschutz und IT Security Merkmalen
- Förderung der Zusammenarbeit mit **Datenschutzbehörden**
- Keine **Rückverfolgung** von personenbez. Daten
- **Beschränkung** der Verarbeitung personenbezog. Daten
- **PIA** (Privacy Impact Assessment) –
Muster für Datenschutzfolgeabschätzungen
- Ableitung von **Maßnahmen**
- ...

Empfehlung der EU Kommission (09.03.12)

Vorbereitung für die Einführung intelligenter Messsysteme

„Empfehlungen“- Auswahl



- **PIA**
- **Privacy by Design / Privacy by Default**
 - Methodische Vorgehensweise ✓
 - 3 Ebenen: legislativ, technisch, organisatorisch (✓)
 - Datenschutzfreundlichste Option → Standardkonfiguration ✓
 - PbD-Referenzarchitektur bevorzugt ✓
- **Grundsätze Datenschutz-Maßnahmen**
 - Datenminimierung ✓
 - Transparenz (✓)
 - Selbstbestimmung (✓)
- **Security** → kryptographische Kanäle ✓
- ...

Empfehlung der EU Kommission (09.03.12)

Vorbereitung für die Einführung intelligenter Messsysteme „Mindestanforderungen“



- für den **Consumer**
 - direkte Bereitstellung ✓
 - enge Zeitintervalle ✓
- für den **Messstellenbetreiber**
 - „Fernablesung“ *(unter Einbeziehung des Datenschutzes)* ✓
 - Bidirektionaler Kommunikationskanal (Steuerung/Wartung) ✓
 - Häufige Ablesung → für Netzplanung (✓)
- **Kommerzielle Aspekte**
 - Unterstützung fortschrittlicher Tarifsysteme ✓
 - Fern-Ein-/Ausschaltung der Versorgung und/oder Lastflüsse oder der Strombegrenzung. ➔ *EM-GW*
- **Security / Datenschutz**
 - sichere Datenkommunikation ✓
 - Verhinderung / Aufdeckung von Betrug ✓

Sichere „Smart Energy“ Systeme: Status

- EnWG 
- Empfehlung der EU Kommission 
- Smart Meter PP 
- Smart Meter Sicherheitsmodul PP 
- BSI TR-03109 "Smart Meter"
 1. PKI 
 2. Kryptographische Vorgaben 
 3. Sicherheitsmodul 
 4. Kommunikationssystem 
- **Energiemanagement** 
- Weitere Standardisierungen bzgl. IT Security im Smart **X** 

KOMPLEXITÄTSFALLE

Vielen Dank!

TÜV Informationstechnik GmbH

Unternehmensgruppe TÜV NORD



Markus Bartsch
IT Security

Langemarckstr. 20
45141 Essen
Germany

Phone: +49 201 8999 – 616
Fax: +49 201 8999 – 666
E-Mail: m.bartsch@tuvit.de
URL: www.tuvit.de



Quellen:

https://www.bsi.bund.de/DE/Themen/SmartMeter/smartmeter_node.html
<http://www.daprim.de>
<http://csrc.nist.gov/publications/PubsNISTIRs.html>
<http://fm4.orf.at/stories/1693989/>
<http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/>