

E-Energy - Smart Grid made in Germany

**von der Vision zur branchen-
übergreifenden Realisierung**

Querschnittsthema

Informationssicherheit

- Schutz der Privatsphäre / Datenschutz
- Eichrechtlicher Anforderungen
- ordnungsgemäße Geschäftsführung

Mainz; 20.April 2010



**E-Energy
Markt Dienstleistung
Use Case**

Indirekte Geräte/Anlagensteuerung durch Anreizsteuerung

- Informationsfluss neuer Anreize

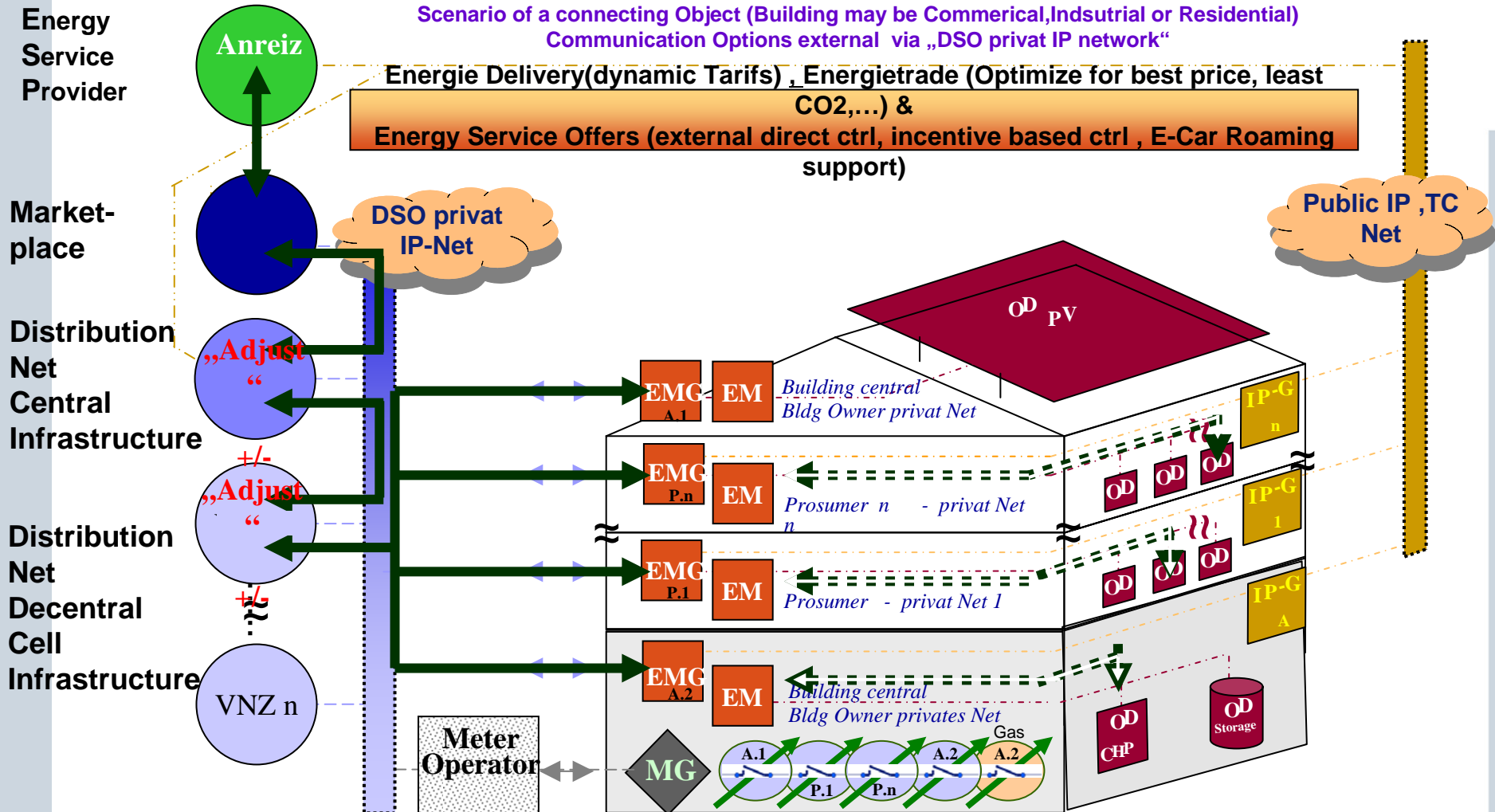
(Ökologisch – CO₂ Anteil, Ökonomisch - Tarife für Wirk und Blindleistung)

bzw Anreizkurve über Zeit

„push broadcast“

Indirekte (Anreiz-) Steuerung

Scenario of a connecting Object (Building may be Commerical, Industrial or Residential)
Communication Options external via „DSO privat IP network“



Energy Delivery (dynamic Tariffs), Energietrade (Optimize for best price, least CO₂,...) & Energy Service Offers (external direct ctrl, incentive based ctrl, E-Car Roaming support)

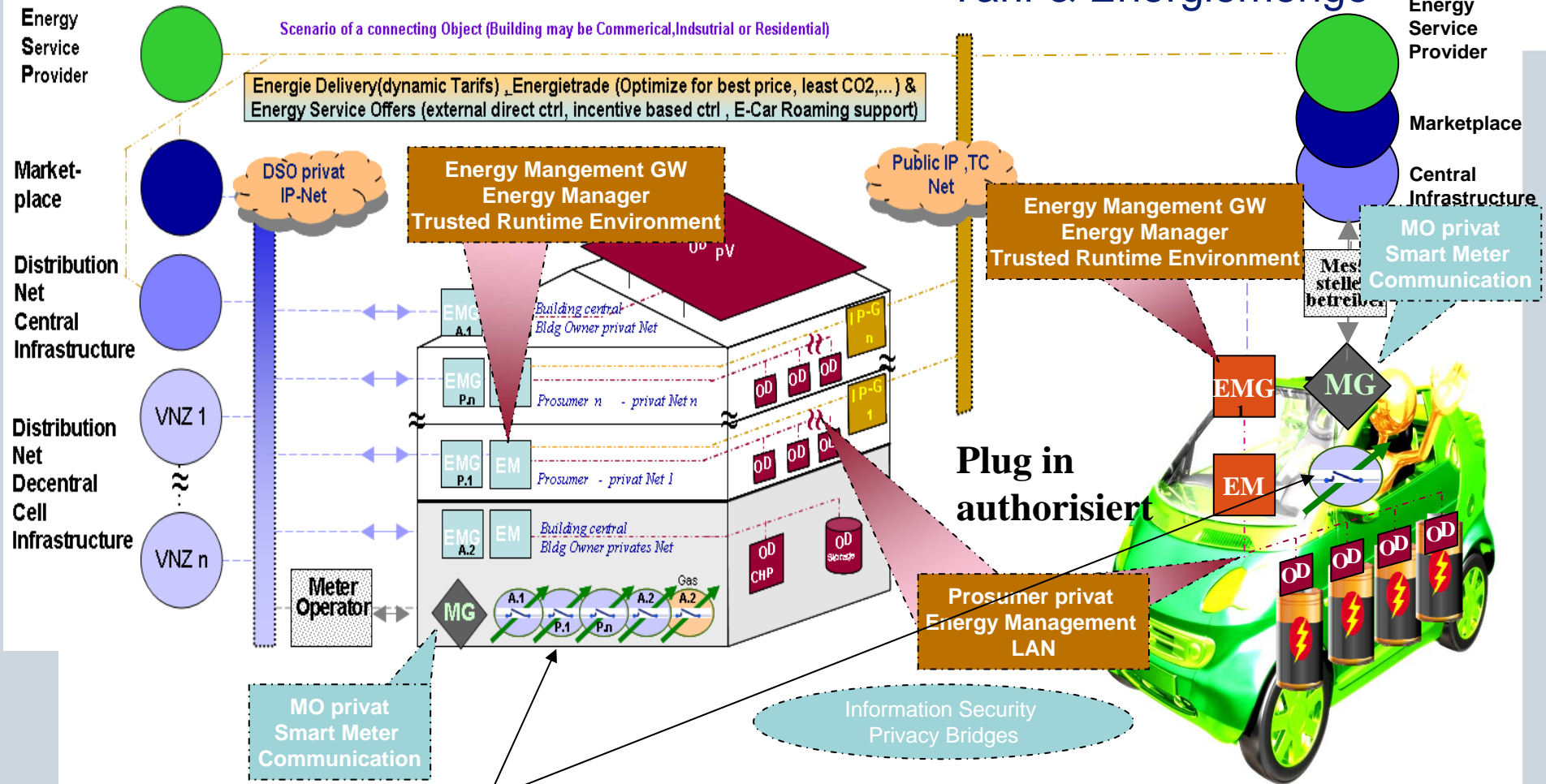
- MG = Meter Gateway
- EMG = Energy Management Gateway
- EM = Energie Manager (Dirigent)
- OD = Objekt Device (gesteuerter Erzeuger/Abnehmer)

**E-Energy
Markt Dienstleistung
Use Case**

**Besuch eines „mobilen/roaming“ Prosumers
z.B. Elektromobiles**

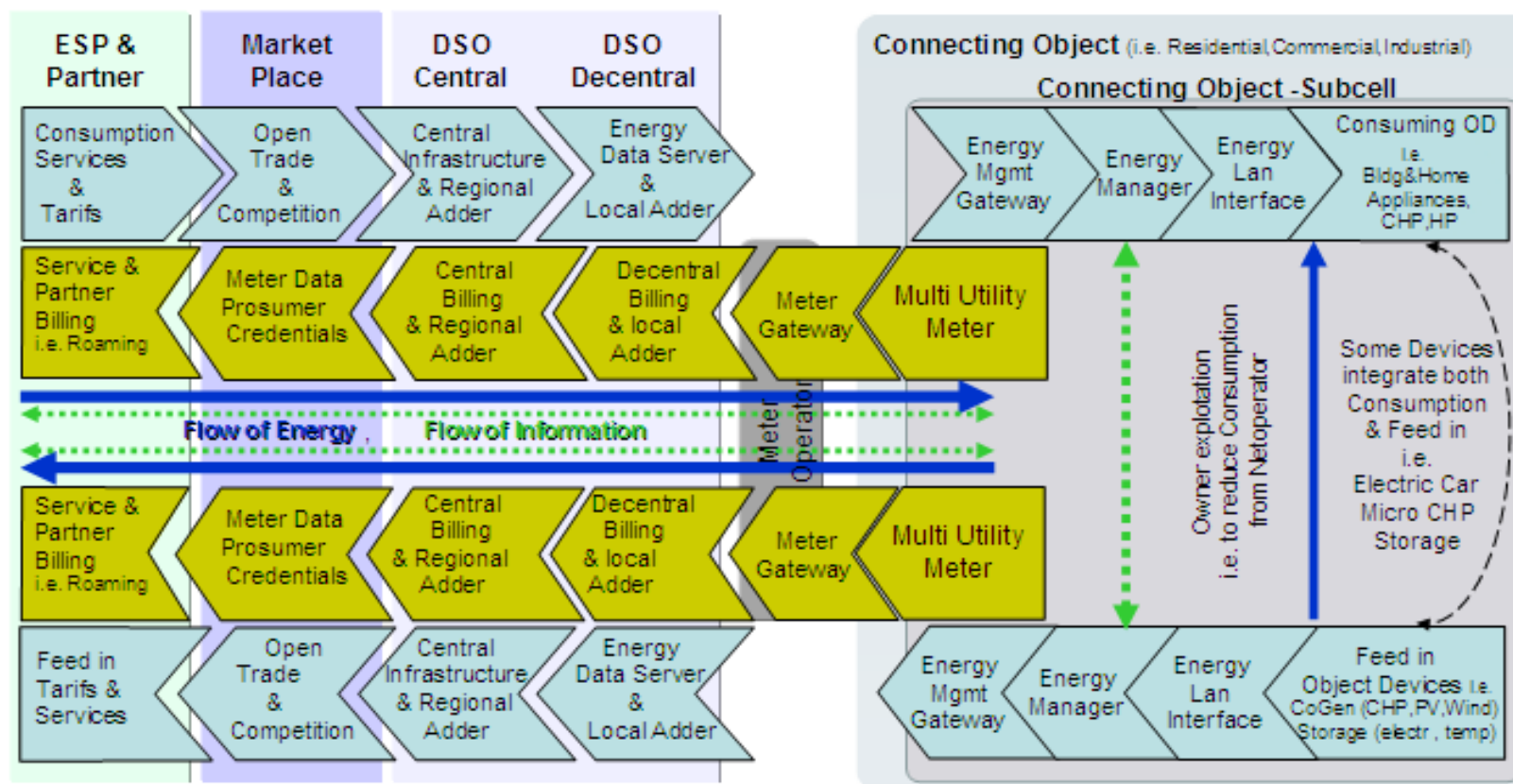
E-Energy noch ein Anwendungsszenario „Besuch eines „mobilen/roaming“ Prosumers Elektromobiles

Tarif & Energiemenge

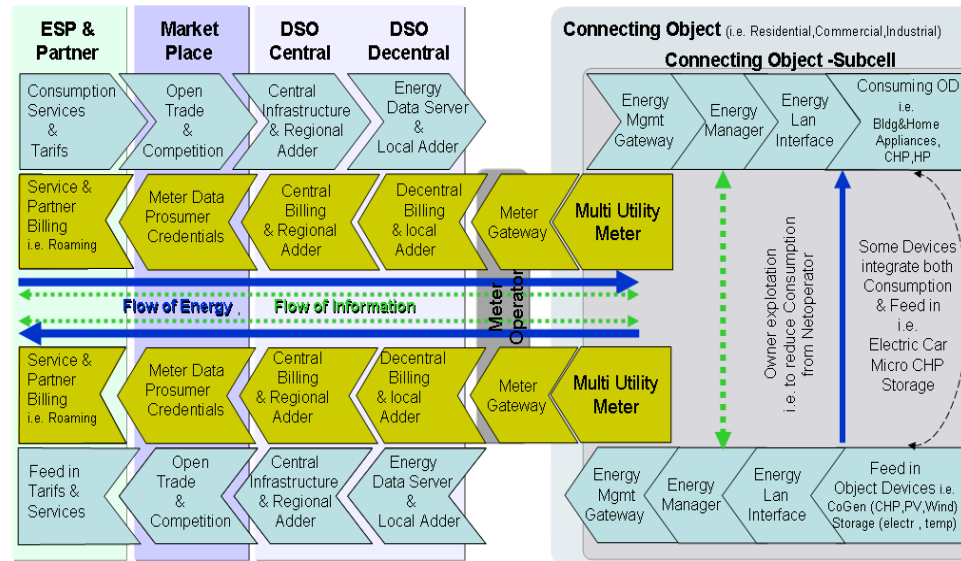


DKE Kompetenzzentrum E-Energy Fokusgruppe Inhouse Automation

Smart Grid & Smart Meter Wirkungsdomänen



Für die Interaktion benötigen die einzelnen Wirkungsdomänen gleichartige Elemente



Teils beschrieben oder in Arbeit

Zielsetzung, einheitliche Funktionsdefinition

1: Basic Connectivity

2: Network Interoperability

3: Syntactic Interoperability

4: Semantic Understanding

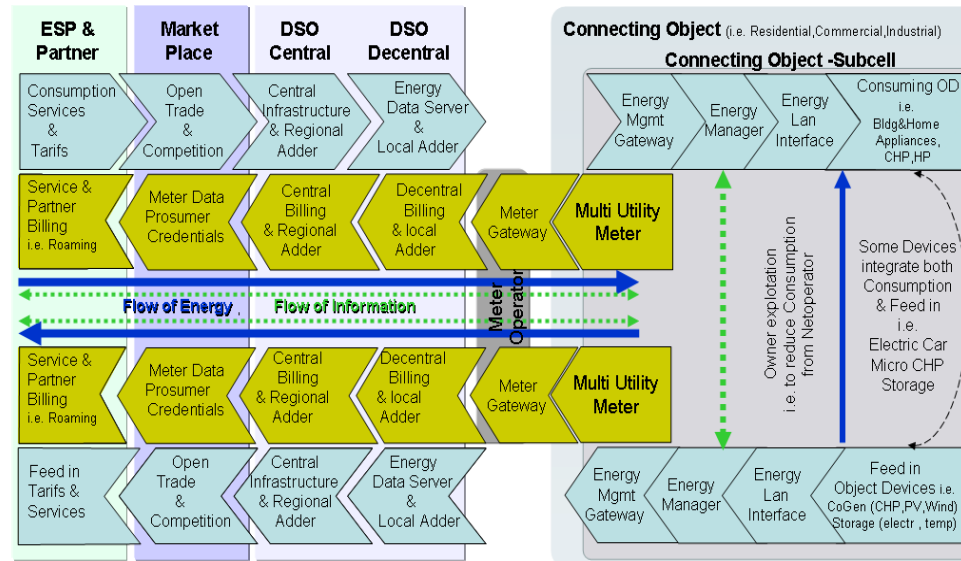
5: Use Case (Geschäftsablauf)

6: Funktionen

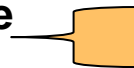
7: Business Objectives

8: Economic/Regulatory Policy

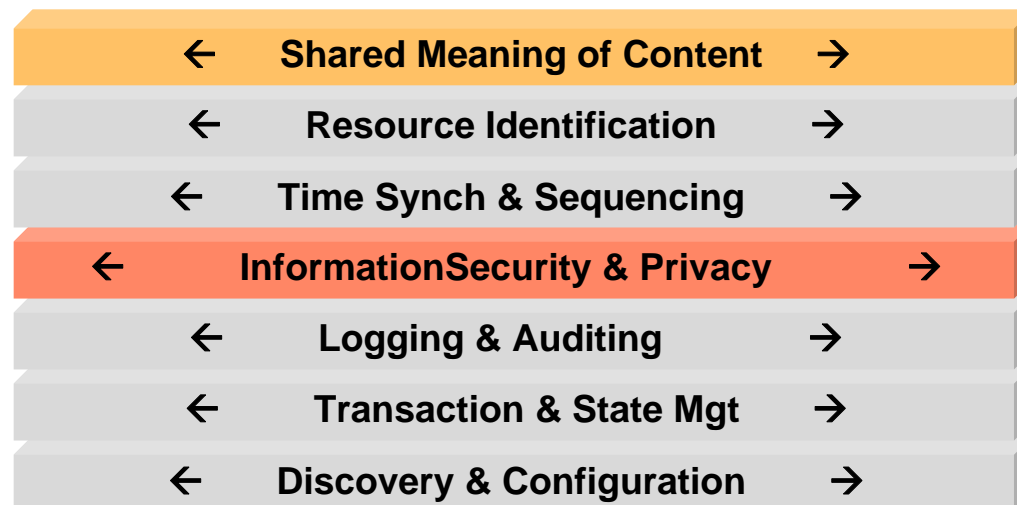
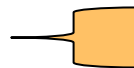
**Horizontale ,
nicht funktionale
Querschnitts-
anforderungen**



**Funktions&Use Case
Beschreibungen**

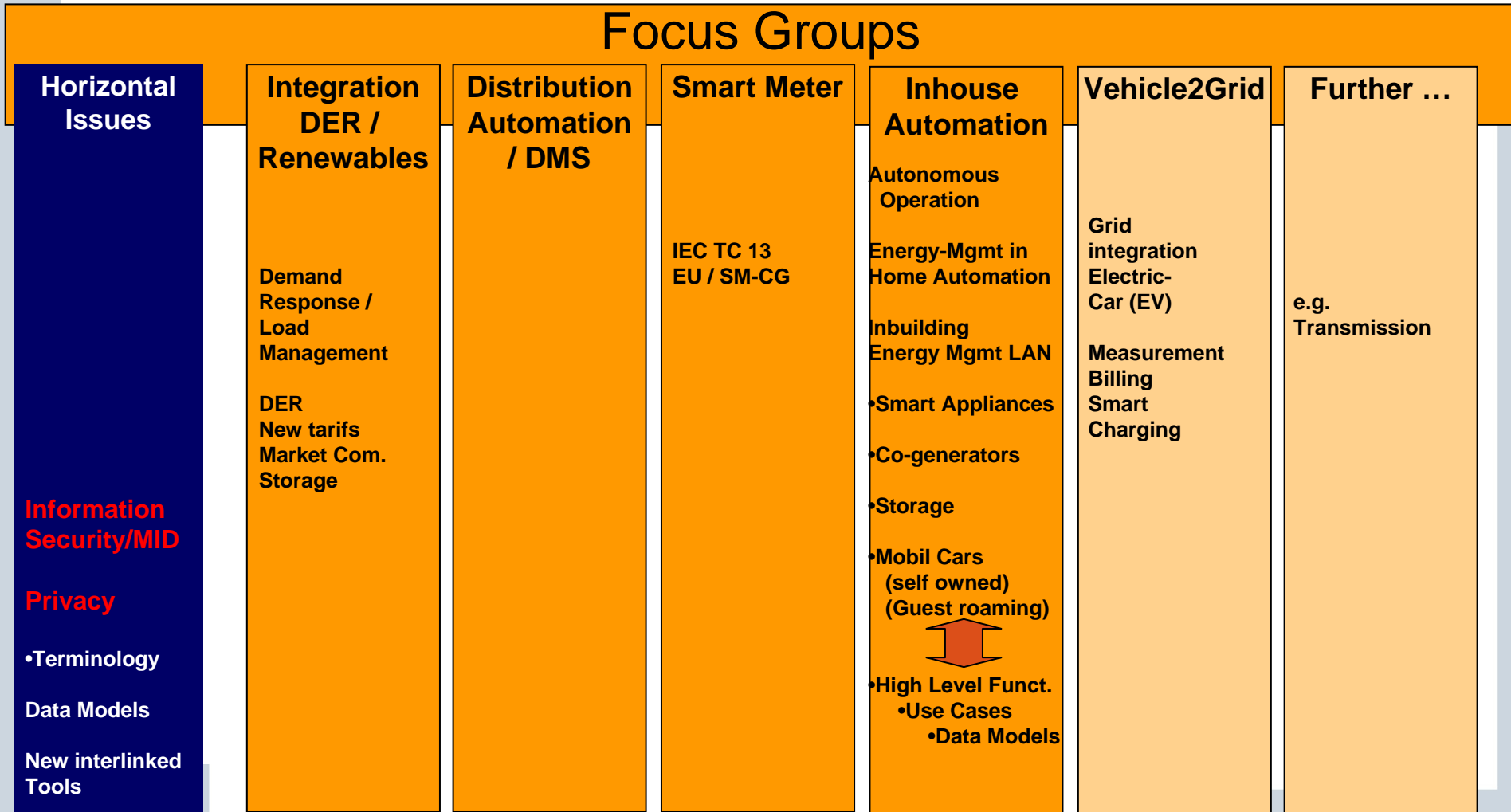


Fokusthema



Steering Committee „Smart Grid and Standardisation“

Focus Groups



und Reaktorsicherheit



Interaction between Focus Groups

Center of Competency for E-Energy

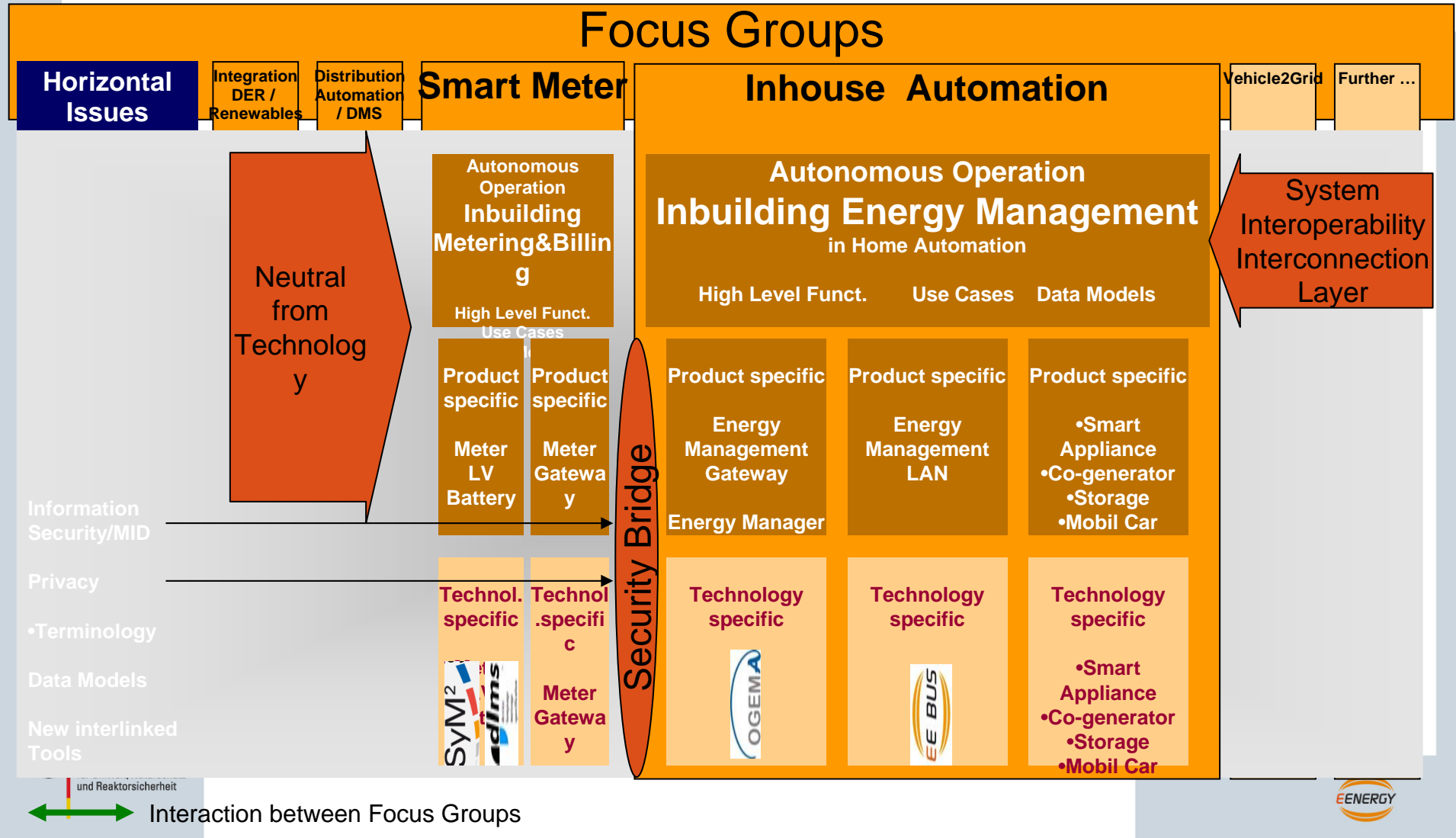
smart Grid made in Germany



Focus Group "Inhouse Automation" – Organisation

Modellstadt Mannheim

Steering Committee „Smart Grid and Standardisation“



Center of Competency for E-Energy

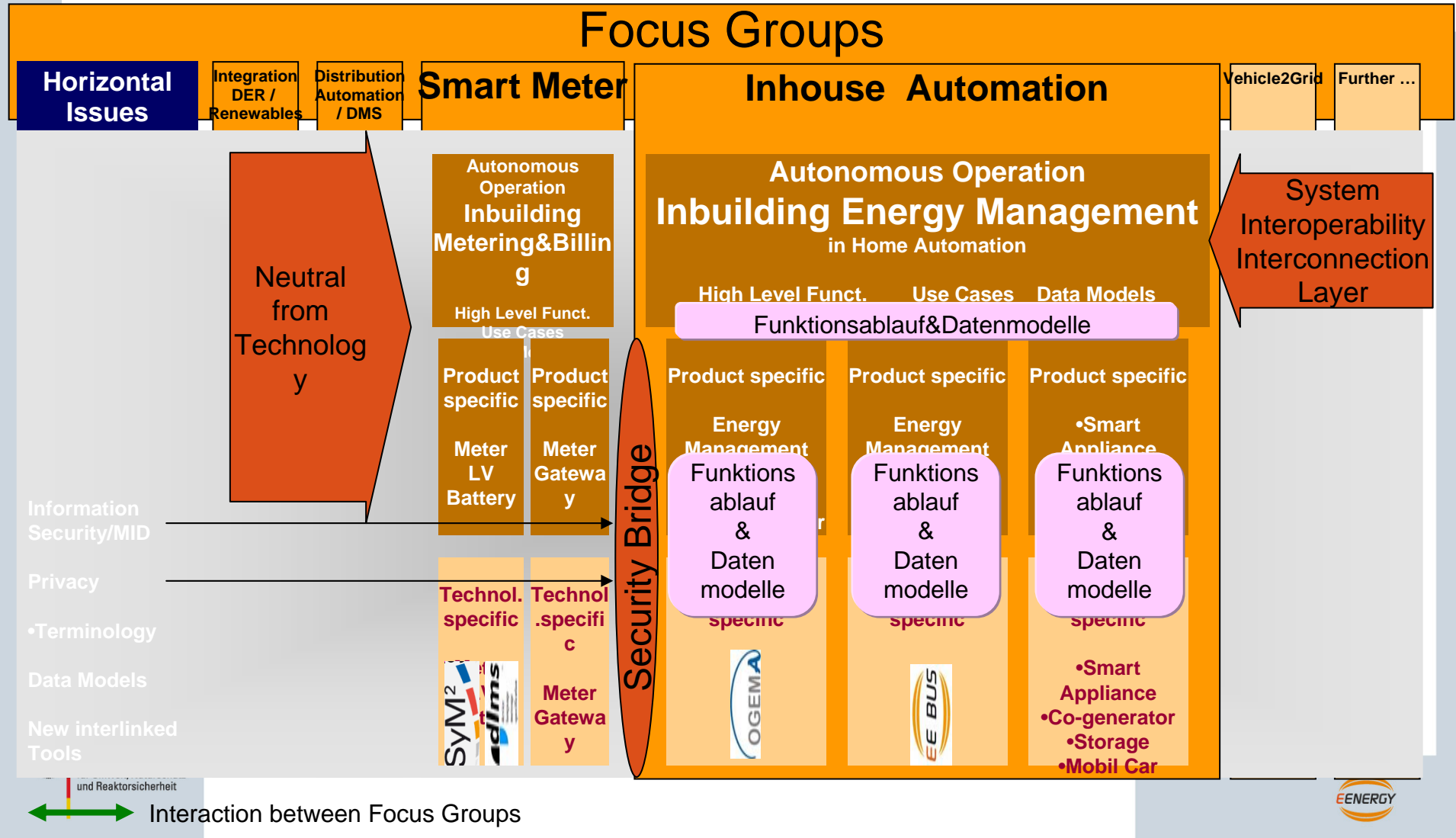
smart Grid made in Germany



Focus Group "Inhouse Automation" – Organisation

Modellstadt Mannheim

Steering Committee „Smart Grid and Standardisation“



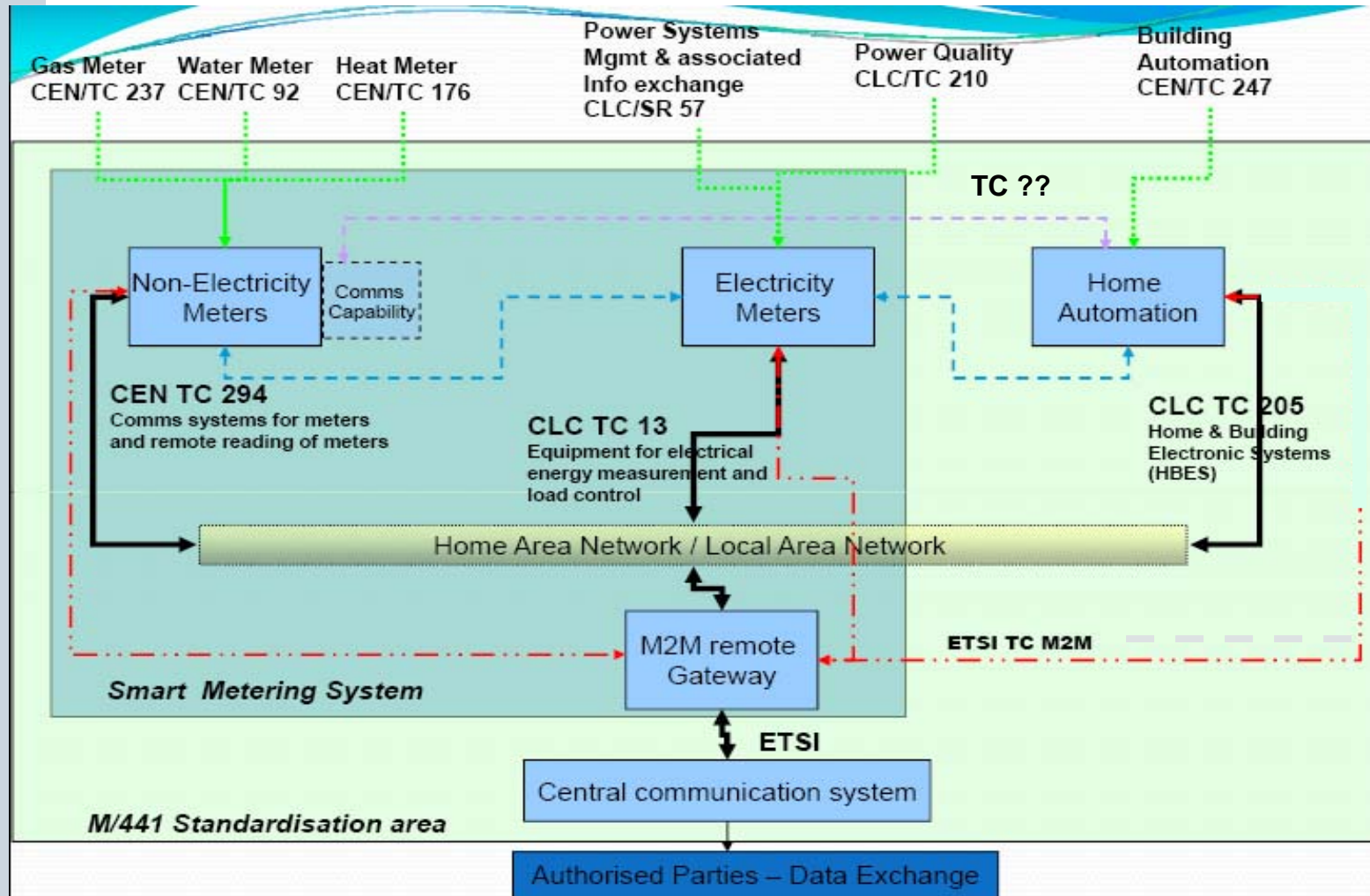
DKE Kompetenzzentrum E-Energy

Fokusgruppe Inhouse Automation

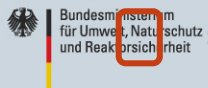


Modellstadt Mannheim

Architekturbild der Smart Meter Coordination Group



Gefördert durch das



= logische Komponenten / Anforderungen



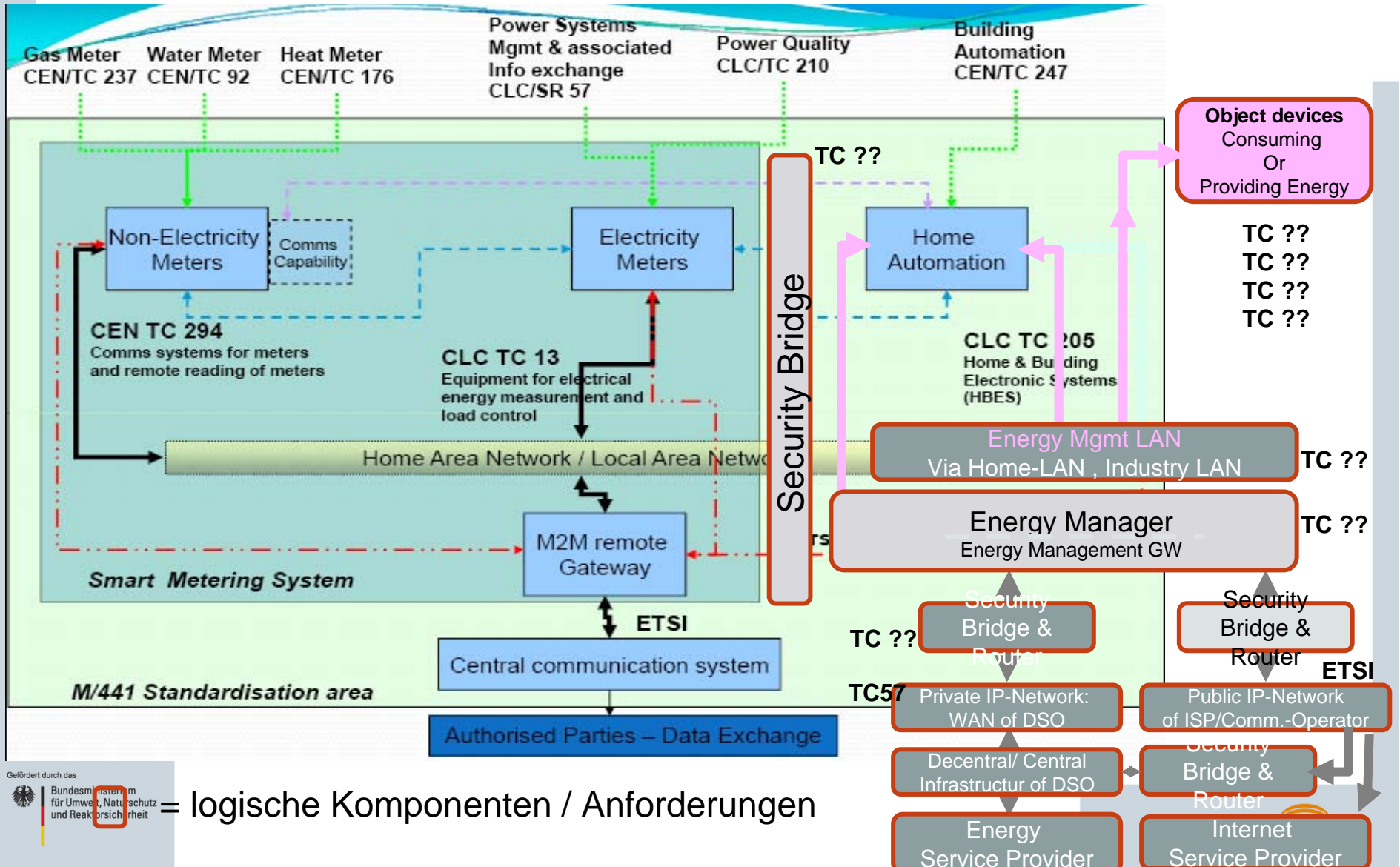
DKE Kompetenzzentrum E-Energy

Fokusgruppe Inhouse Automation

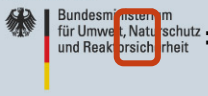


Modellstadt Mannheim

Architekturbild der Smart Meter Coordination Group- Updates FG Inhouse Automation

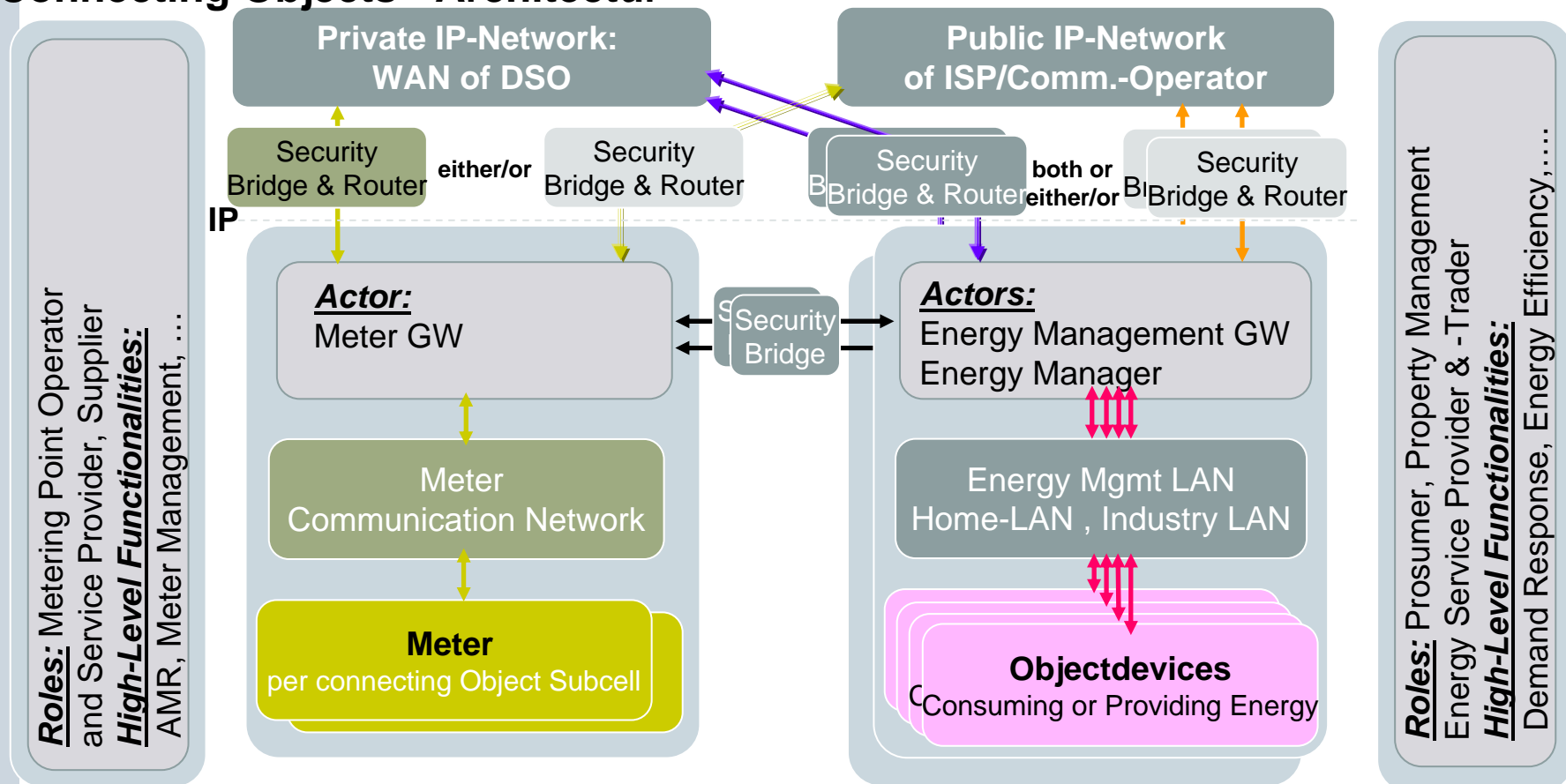


Gefördert durch das



= logische Komponenten / Anforderungen

Connecting Objects - Architektur



Roles: Metering Point Operator and Service Provider, Supplier
High-Level Functionalities: AMR, Meter Management, ...

Roles: Prosumer, Property Management Energy Service Provider & -Trader
High-Level Functionalities: Demand Response, Energy Efficiency, ...

Domain: Connecting Object (Building)
Actors: Equipment for energy measurement (MID) (Electricity and Non-Electricity Meters)

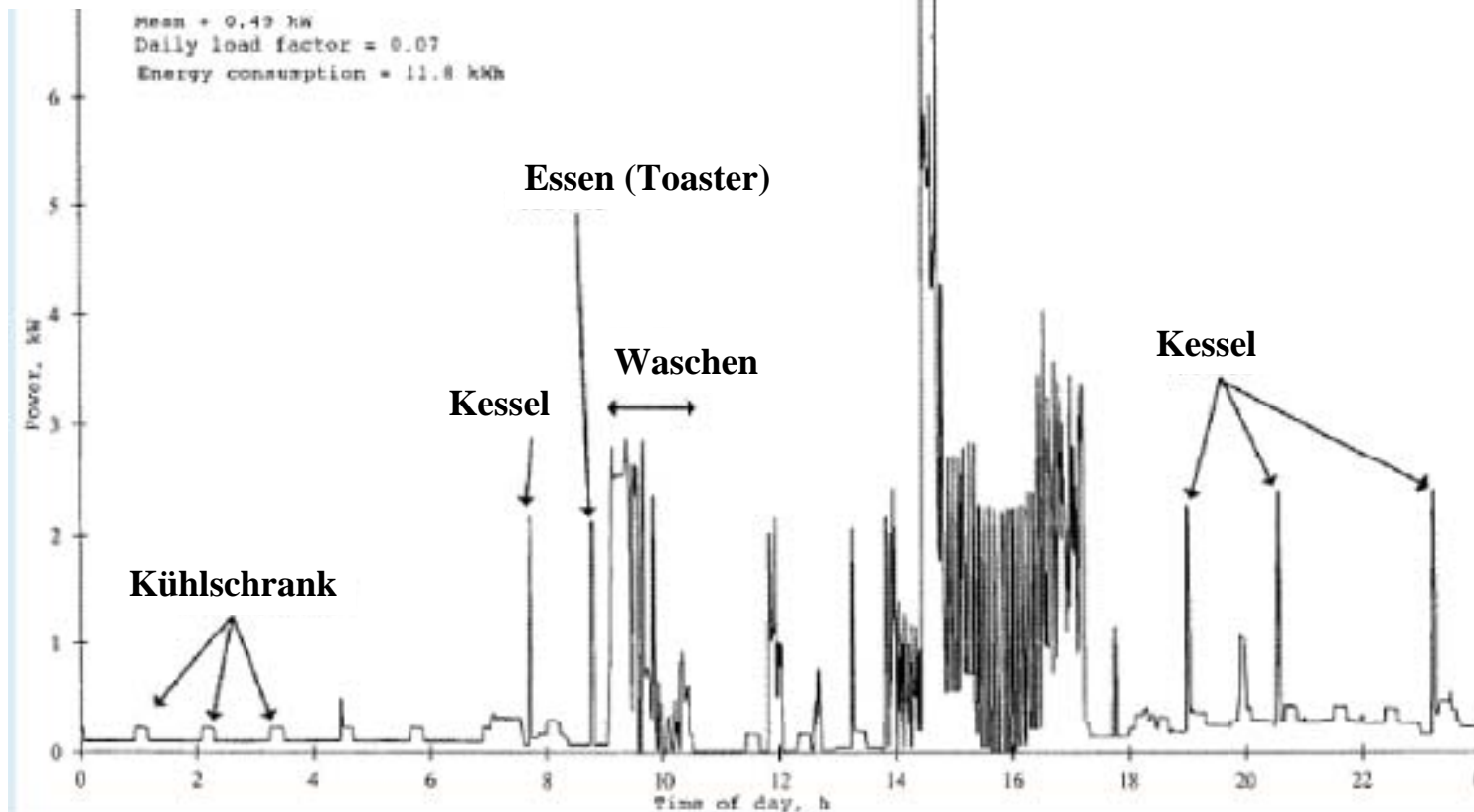
Domain: Inhouse Automation
Actors: Building&Home Electronic Systems (Sensors/Actuators, Energy Consumers(Appliances) Energy Generators / Storages)

Herausforderung Zellularer Ansatz

**Netzwerk basierend
Energetisch und kommunikativ
verschiedene Privatsphaeren**

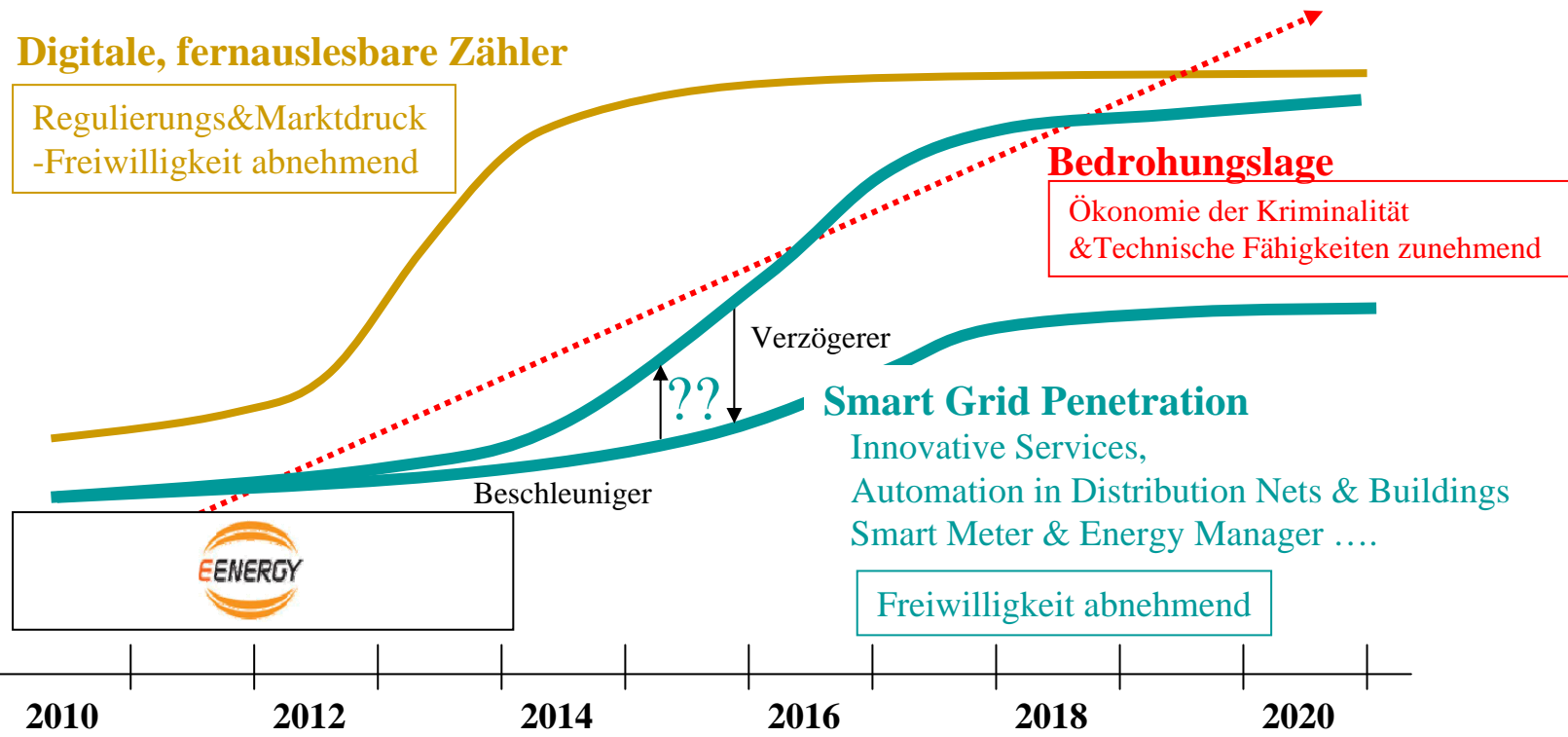
**Bidirektionaler Energie Austausch
Bidirektionaler Daten Austausch
Über Systemgrenzen hinweg
Über verschiedene rechtliche Einheiten
Zwischen verschiedenen Privatnetzen**

Persönliche Verhaltensweisen „Beschäftigungskategorien und Profile“ An- / Abwesenheit



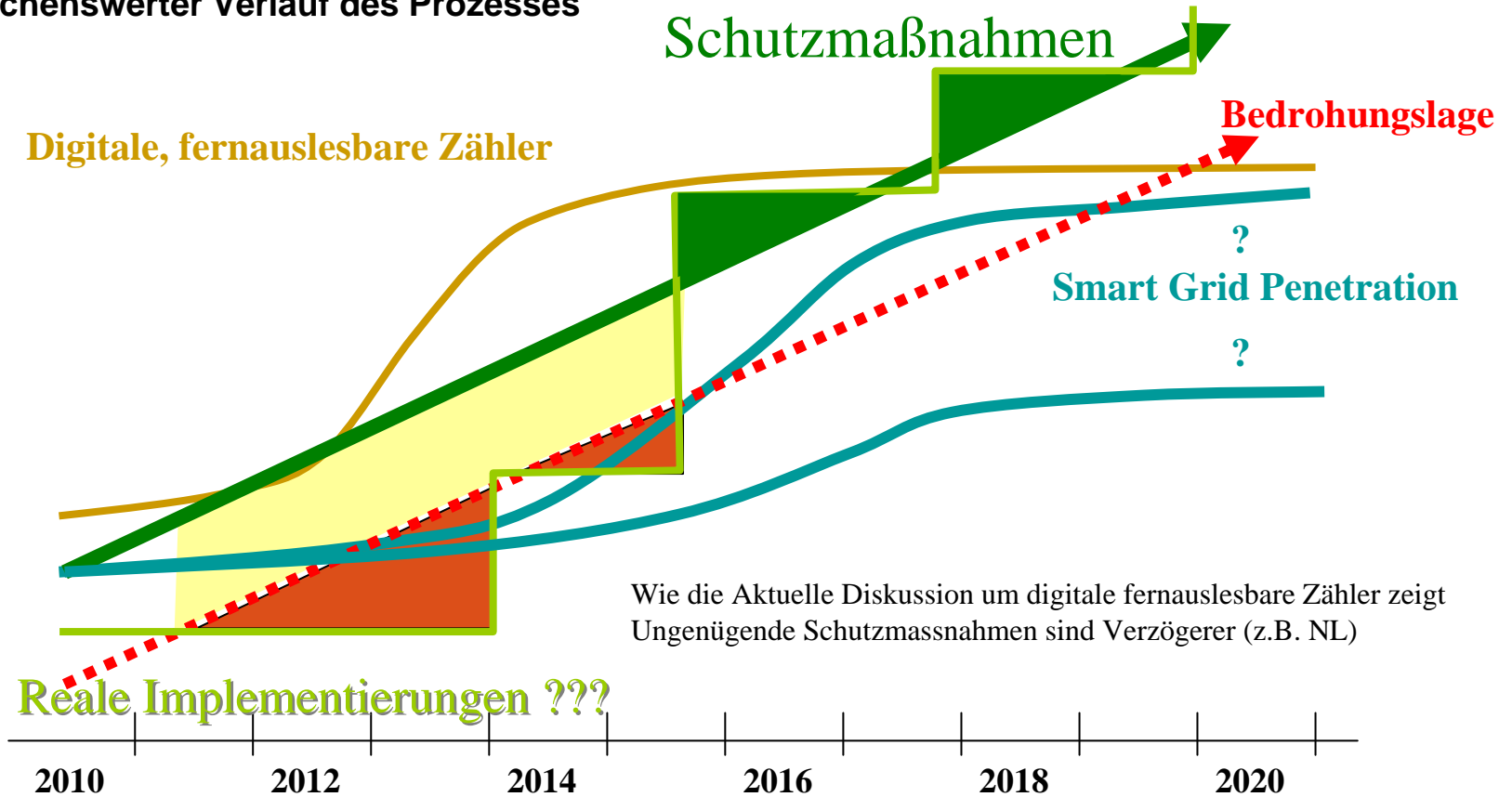
Quelle: Elias Leake Quinn, [Smart Metering & Privacy: Existing Law and Competing Policies](#), Frühjahr 2009, S. 3.

Angriff vs. Verteidigung – Eine Ungleichung



Schutz und Bedrohung – ein Rennen

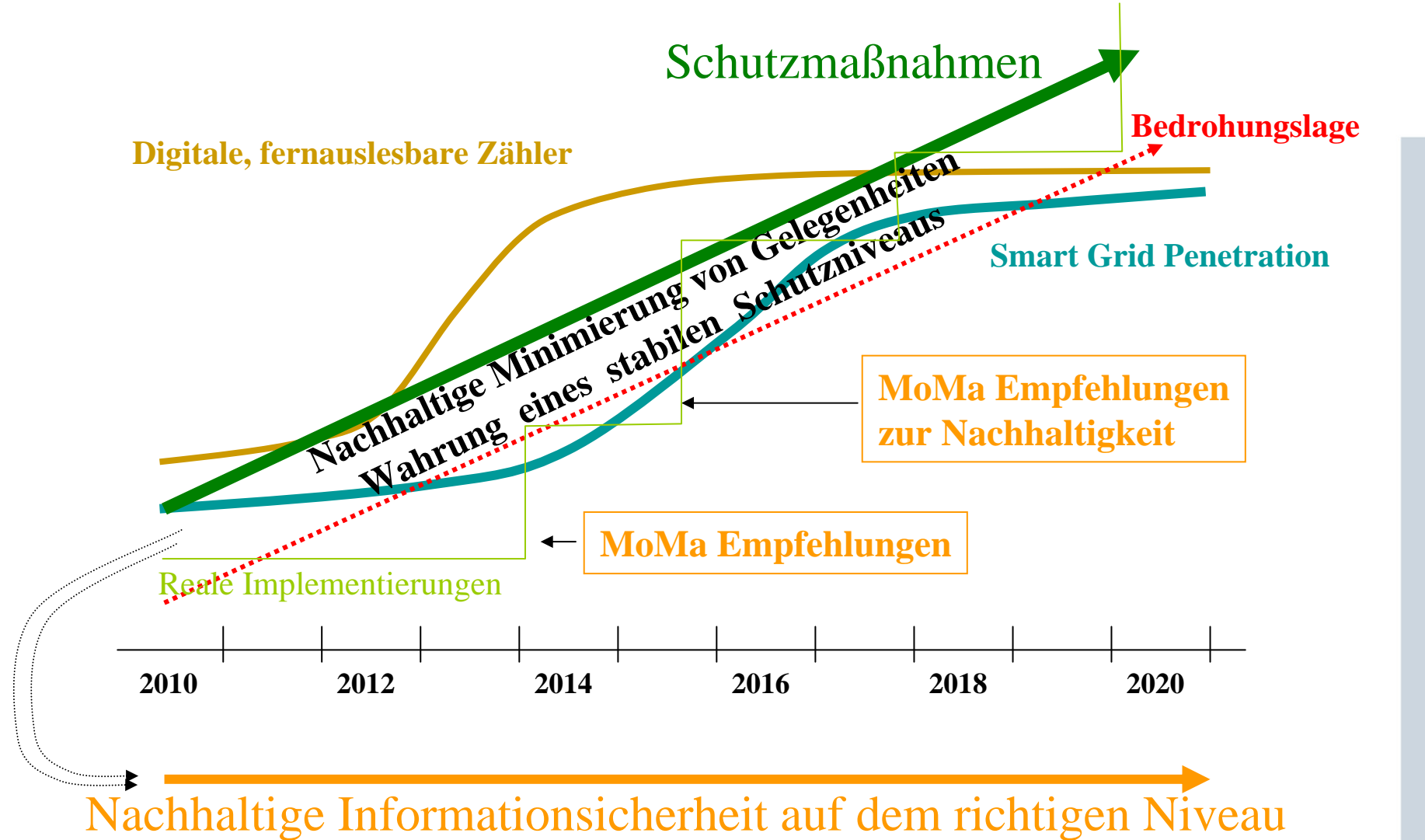
– wünschenswerter Verlauf des Prozesses



- Nicht akzeptabel
- Risikoreich
- Vertrauenswürdig

Schutz und Bedrohung – ein Rennen

– wünschenswerter Verlauf des Prozesses



- ▶ Lessons Learned aus anderen Sektoren !
 - ▶ **Die schwächsten Glieder bestimmen das Gesamtsystem**
 - ▶ **die Akzeptanz ist von einer durchgehenden Lösung abhängig**

- ▶ In „MoMa“ wurden verschiedene Szenarien betrachtet daraus ergaben sich viele Herausforderungen an die Informationssicherheit

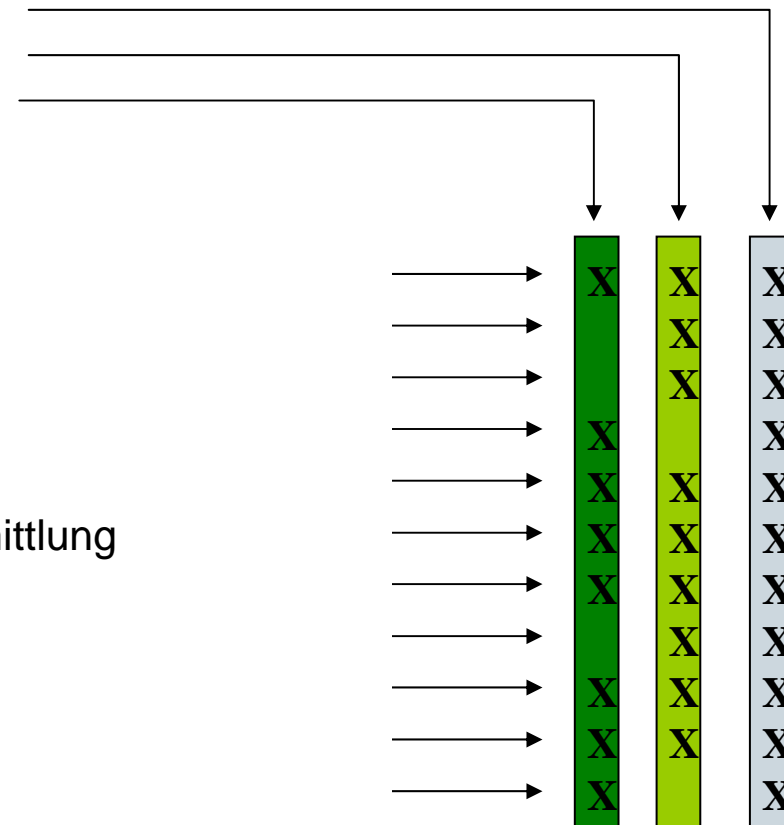
- ▶ Es muss durchgängig im **Gesamtsystem** gewährleistet werden d.h. bei alle „Physikalischen und Logischen Systemkomponenten“

- ▶ Analysen der vorhanden Normen
 - ▶ Energiesektor
 - existierende Lösungen für die Smart Grid-Kernarchitektur
 - IEC 62351
 - BDEW-Weißbuch zum Thema „Sicherheit für den Netzbetrieb“
 - ▶ Informations & Telekommunikationssektor
 - ▶ BNETZA Empfehlungen
 - ▶ Kompass der IT Sicherheit DIN/BITKOM

- ▶ **Nationale Festlegungen erschweren globale Harmonisierung**

Grundlegenden Sicherheitsanforderungen sind einzuhalten

Ordnungsgemäße Geschäftsführung
Datenschutz
Eichrecht



- ▶ Authentizität
- ▶ Nutzungsfestlegung
- ▶ Vertraulichkeit
- ▶ Integrität
- ▶ Authentifizierung
- ▶ Rechtsicherheit der Datenübermittlung
- ▶ Revisionsicherheit
- ▶ Datenschutz
- ▶ Legitimität
- ▶ Valitität
- ▶ Verfügbarkeit

- letzteres beinhaltet Funktionsfähigkeit der Systeme & Komponenten

Querschnittsthema

Informationssicherheit und Datenschutz/Schutz der Privatsphäre

– incl. Eichrechtlicher Anforderungen



Modellstadt Mannheim

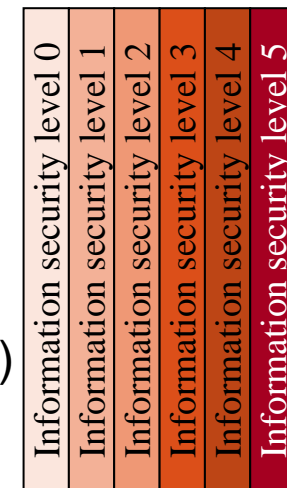
Zielstufen definiert für Informationssicherheit und Datenschutz

moma „Security Klassen“

Festlegungen aus existierenden Normen

für folgende Elemente der Sicherheitsinfrastruktur und deren Schutzniveaus

- ▶ Verschlüsselung (Algorithmen, Hardware)
berücksichtigen Empfehlungen der BNetzA (für 2015)
- ▶ Kommunikationstack
- ▶ Logging, Daten (+Datentiefe)
- ▶ Anwendung/Services (Zugriffstiefe, Authentifizierung)
- ▶ die Benutzer / Rollen / Gruppen (Zugriffstiefe, Authentifizierung)
- ▶ Räumlichkeiten(physikalischer Schutz)



MoMa Spektrum

Querschnittsthema

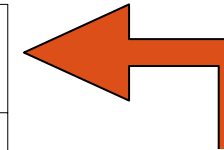
Informationssicherheit und Datenschutz/Schutz der Privatsphäre

– incl. Eichrechtlicher Anforderungen



Modellstadt Mannheim

Security Level 3	Informationssicherheitsniveau „HOCH“ Für alle schützenswerten Daten
Verschlüsselung (Algorithmen, Hardware)	Verschlüsselung mindestens entsprechend der Empfehlung der Bundesnetzagentur für 2015 bezüglich: Hashfunktionen , Signaturverfahren, Zufallsgenerator
Kommunikation- stack	Kommunikation verschlüsselt - mindestens entsprechend der Empfehlung der Bundesnetzagentur , nur dedizierte Ports offen + privates gesichertes Netzwerk
Logging	Application Logging und Zugriffs Logging, Logs gegen Manipulation geschützt
Daten (+Datentiefe)	Daten verschlüsselt mindestens entsprechend der Empfehlung der Bundesnetzagentur, nur notwendige Daten verfügbar für authentifizierten Benutzer
Anwendung	Kein Zugang zu den Systemdaten und eingeschränkter Zugang zu Anwendungsdaten, gegenseitige Authentifizierung mittels Zertifikaten
Benutzer/Rollen / Gruppen	Kein Zugang zu den Systemdaten, eingeschränkter Zugang zu Anwendungsdaten, gegenseitige Authentifizierung mittels Zertifikaten (Softwarezertifikate)
Raum	Physikalischer Schutz Kontrollierter, zugangsgesicherter Raum (logging)



**Stand der
Technik
2015**



MoMa Spektrum

Querschnittsthema

Informationssicherheit und Datenschutz/Schutz der Privatsphäre

– incl. Eichrechtlicher Anforderungen



Modellstadt Mannheim

Zielstufen definiert für Informationssicherheit und Datenschutz

- ▶ **moma Datenklassen** beinhalten Schutzniveaus – **aus vorhandenen Normen**

- ▶ Personenbezogene Daten und
- ▶ Persönliche Daten
(hieraus kann persönliches Verhalten abgeleitet werden)
- ▶ Steuerungsdaten
- ▶ schützenswerte Vertrags- und Abrechnungsdaten
- ▶ Allgemeine Daten

Gefördert durch das



Bundesministerium
für Umwelt, Naturschutz
und Reaktorsicherheit



Querschnittsthema

Informationssicherheit und Datenschutz/Schutz der Privatsphäre

– incl. Eichrechtlicher Anforderungen

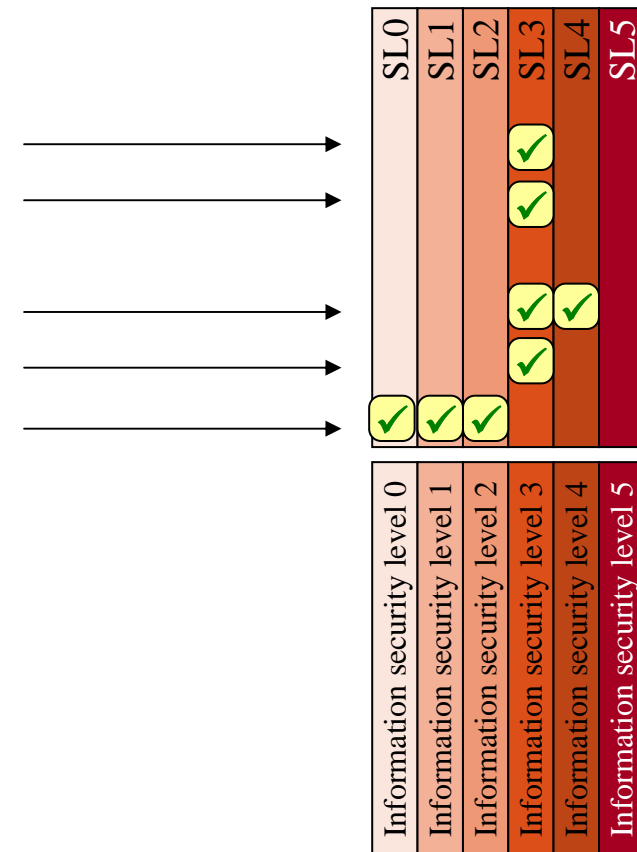


Modellstadt Mannheim

Zielstufen definiert für Informationssicherheit und Datenschutz

► **moma Datenklassen** beinhalten Schutzniveaus – **aus vorhandenen Normen**

- Personenbezogene Daten und
- Persönliche Daten
(hieraus kann persönliches Verhalten abgeleitet werden)
- Steuerungsdaten
- schützenswerte Vertrags- und Abrechnungsdaten
- Allgemeine Daten



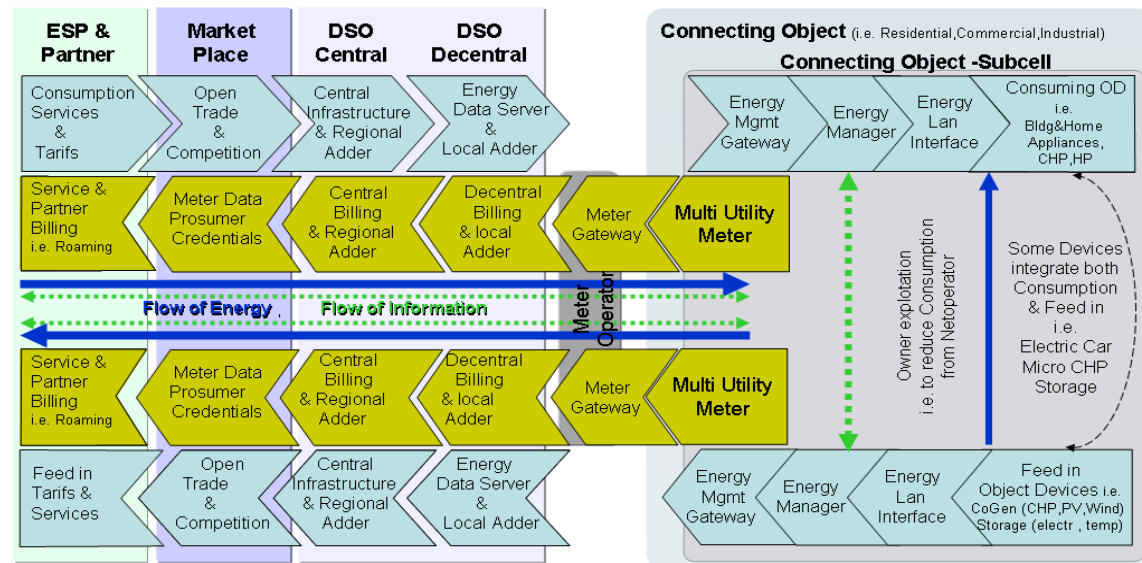
Durchgängige Informationssicherheit

Ordnungsgemäße Geschäftsführung
Datenschutz
Eichrecht

.....
.....

- ▶ Legitimität
- ▶ Authentizität
- ▶ Vertraulichkeit
- ▶ Integrität/Valität
- ▶ Authentifizierung
- ▶ Rechtsicherheit der Datenüberm.
- ▶ Nutzungsfestlegung
- ▶ Datenschutz
- ▶ Revisionsicherheit
- ▶ Verfügbarkeit

- letzteres beinhaltet Funktionsfähigkeit der Systeme & Komponenten



Personenbezogene Daten und Persönliche Daten
Steuerungsdaten
schützenswerte Vertrags- und Abrechnungsdaten
Mandanten Anreize(ökologisch & ökonomisch)
SLAs(Betriebsführung)
Allgemeine Daten

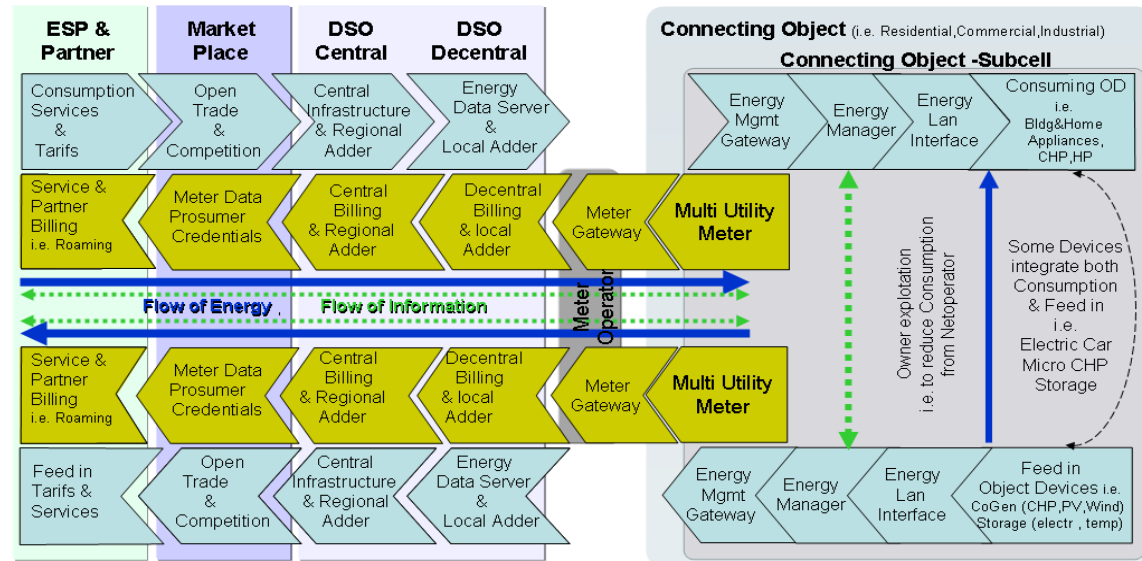
Durchgängige Informationssicherheit

Ordnungsgemäße Geschäftsführung
Datenschutz
Eichrecht

.....
.....

- ▶ Legitimität
- ▶ Authentizität
- ▶ Vertraulichkeit
- ▶ Integrität/Valitität
- ▶ Authentifizierung
- ▶ Rechtsicherheit der Datenüberm.
- ▶ Nutzungsfestlegung
- ▶ Datenschutz
- ▶ Revisionsicherheit
- ▶ Verfügbarkeit

- letzteres beinhaltet Funktionsfähigkeit der Systeme & Komponenten



AAA **Authenticate**, Authorize, Account (Identity Management)
 Verschlüsselung (Algorithmen, Hardware)
 Signiert (Anreizeangebote, Tarife, Abrechnungsrel. Messwerte) End2End
 Kommunikationstack
Anwendung/Services (Zugriffstiefe, Authentifizierung)
Benutzer / Rollen / Gruppen (Zugriffstiefe, Authentifizierung)
 Räumlichkeiten (physikalischer Schutz)
 Logging, Daten (wann, wer, welche Daten+Datentiefe)

- ▶ Verfügbarkeit und Funktionsfähigkeit des Systemes
kein Engpass in der Energieversorgung / Einspeisemöglichkeiten

Wirtschaftliche Verlust da unfähig am Anreizsystem teilzunehmen
Behinderung des Geschäftsablaufes E-Energy Services Vertragstreue

Schwarmverhalten , „Notfall“-Abschaltung von Unterobjektnetzzellen(z.B. Wohnungen) – muss genauer untersucht werden

Betrachtete Angriffsszenarien

Denial of Services, BOTNetze oder durch Drive by Infection, Malware, Patches

- ▶ Speziell an der Schnittstelle (MG & EMG) zwischen Objektnetzzellen & den Verteilnetzzellen bieten heutige Konzepte und "best practises" der Systemkomponenten keinen **nachhaltigen Schutz** vor Angriffen auf die Verfügbarkeit, bzw der Privatsphäre

Querschnittsthema

Informationssicherheit und Datenschutz/Schutz der Privatsphäre

– incl. Eichrechtlicher Anforderungen



Modellstadt Mannheim

- ▶ **Erkannte Schwachstellen - Handlungsbedarf**
 - ▶ Metergateway / Meter
 - ▶ verschiedene Aspekte & Nachhaltigkeitsanforderungen
 - ▶ **Opt out Möglichkeiten und deren Kontrolle**

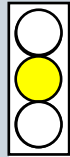
- ▶ **Energiemanagement Gateway/ Energie Manager – trusted Runtime Computing Platform**

- ▶ **Dezentrale Verteilnetzzellen Server** – verschiedene Aspekte

- ▶ Anforderungen aus Eichrecht (Gesamtsystem) – und Datenschutz

Weiterhin Nachhaltigkeit in Bezug auf

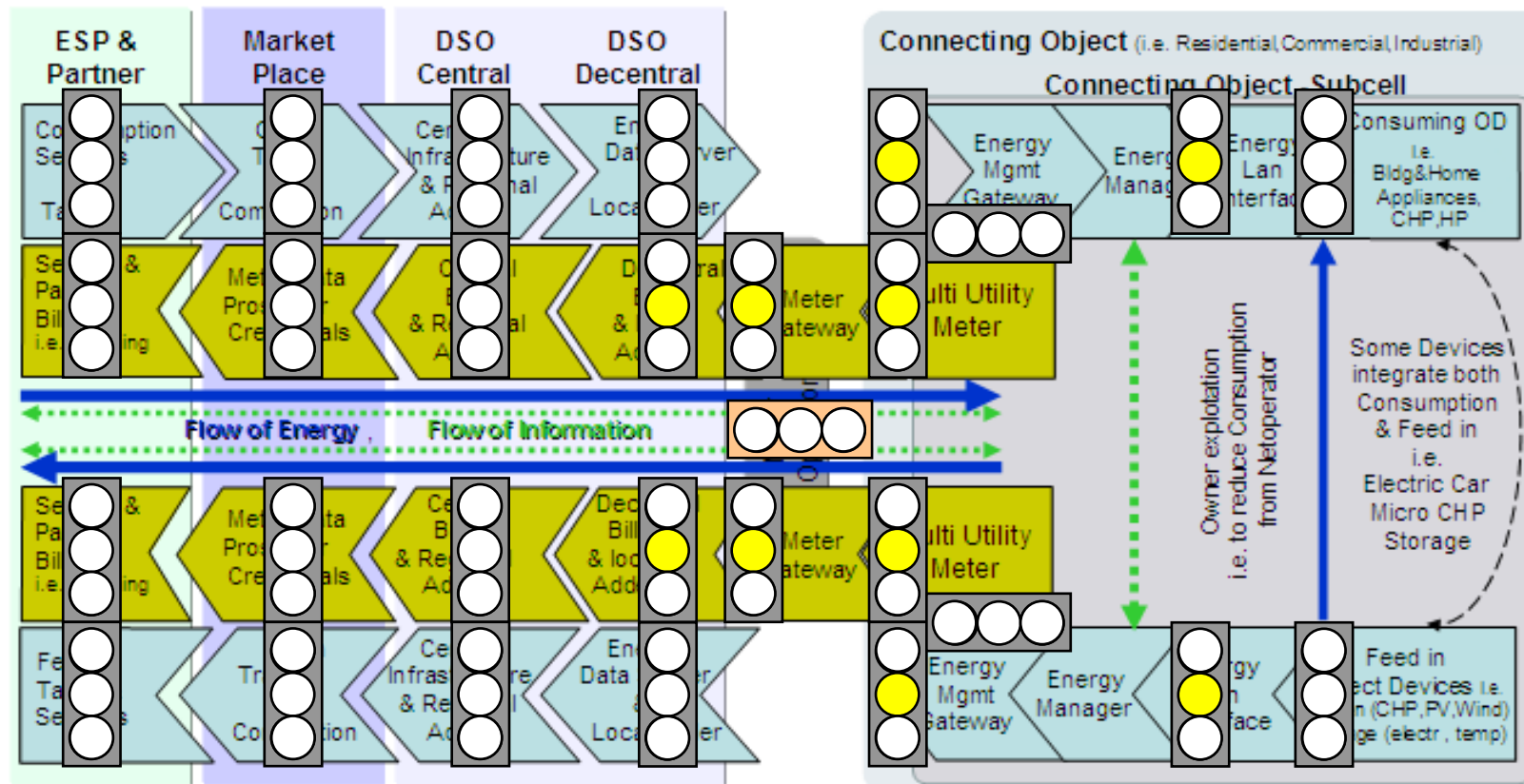
- ▶ Elektromobilität & Roaming
- ▶ Prosumer Hoheit über gespeicherte Daten & Kontrolle der Vertraglichen Regelungen
- ▶ Langfristige Anpassungsoptionen der Infrastruktur der Informationssicherheits (Was tun wenn Schlüssel kompromitiert wurden - Reaktionszeit)
- ▶ Erhöhung des Schutzniveaus über Zeit (Anpassungszyklus eher klein)



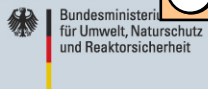
Gesamtsystem

DKE Kompetenzzentrum E-Energy Fokusgruppe Inhouse Automation

Smart Grid & Smart Meter Wirkungsdomänen



Gefördert durch das



Bundesministerium
für Umwelt, Naturschutz
und Reaktorsicherheit

Technisch

Organisatorisch

▶ **Langfristige NACHHALTIGKEIT**

Mit hoher Penetration der E-Energy Lösungen steigen die Bedrohungspotentiale und damit die Anforderungen an die Informationssicherheit !

Vertrauen und Sicherheitsniveau auch langfristig halten -> Investitionen in Digitale, fernauslesbare Zähler

▶ **Einsatz moderner „Smart Cards“** oder ähnlicher Konzepte erscheint nachhaltig

- Erhöhung der Benutzerfreundlichkeit und Akzeptanz
vermittelbares und impliziertes Vertrauen in E-Energy Services und Angebote
- Abdeckung der Anforderungen aus dem Eichrecht

Trennung zwischen installierten Systemkomponenten
von sicherheitsrelevanten Anforderungen an

Verschlüsselungen, Authentifizierungen & Signierungen der Daten

- Bietet langfristigen update Möglichkeit und damit „Investitionsschutz“
bei den installierten Systemkomponenten (MG, Meter EMG , EM
- **notwendig bei offenem Markt**
Einführung einer Mandanten / vertragsabhängigen Verschlüsselung.
- **notwendig bei Elektromobil Szenarien zum roaming & kommunizieren Host / Gast**
- kann die Anreicherungen und Bündelung von Angebote erleichtern, Authentifizierung kann
mittels dieser Smart Card auch bei neuen Services verwendet

Übergreifendes Informationssicherheits Management System

Informationssicherheits „Response Center“ / „Protection Center“

- ▶ Erkennen ob häufiger als zur Abrechnung relevant erfasst (Nicht vertragsgemässe Zwischenablesungen)
- ▶ Erkennen wann was kompromittiert wurde (anonymisierte Analyse)
 - ▶ Eingreif managment - was tun wenn / in welcher Zeit
 - ▶ Patchmanagment – schliessen der Lücken im Gesamtsystem
 - ▶ Pflichtpachtes – sicherstellen
 - ▶ Remote Managment
- ▶ SmartGrid Remote Access
- ▶ Identitäts- und Schlüsselmanagement
- ▶ Verwaltung der Zugriffsauthorisierungen und -tiefen von Aktueren
 - ▶ Rollen / Gruppen /Benutzer
 - ▶ Applilationen
- ▶ Dokumente Lifecycle Management-im Gesamtsystem und bei Konzerntöchtern
 - ▶ Wem gehören Daten
 - in bei Erfassung, in Bewegung, in Nutzung , „at Rest“
 - ▶ Verfügbarkeit – 7/24
 - ▶ Digital Rights Management
 - Zugriffsrechte an Information – kann nur von Berechtigten gelesen werden
 - ▶ Aufbewahrungsfristen
 - ▶ Lösch „policy“ und –anweisungen
 - ▶ Während , nach Auftragsbearbeitung
 - ▶ Kontrolle der Löschungen / Nachweise

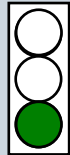
- ▶ Systemkomponente besteht aus Lokationen, Hardware, Betriebssystem, Applikationen, Daten sowie Zugriffsmöglichkeiten zwischen Applikationen&Services, durch Benutzer, Rollen oder Gruppen

- ▶ **Bewertung des Gesamtsystemes ist schwierig**
 - ▶ Vorgehensweisen bei E-Energy Projekten unterschiedlich

- ▶ **Normungsbedarf bezüglich Vergleichbarkeit und Konformität**
„Unified Compliance Framework Profil 1.0“?
 - ▶ Vorschlag : Kombi Methode „Stufenansatz“
 - ▶ Informationssicherheitsstufen
 - ▶ Datenschutzklassen
 - ▶ Datenreichweite
 - ▶ Zugriffstiefen der Applikationen, Benutzer, Rollen bzw Gruppen
 - ▶ Normaler Betrieb / Fernzugriff
 - ▶ Wartung / Updates

Querschnittsthema

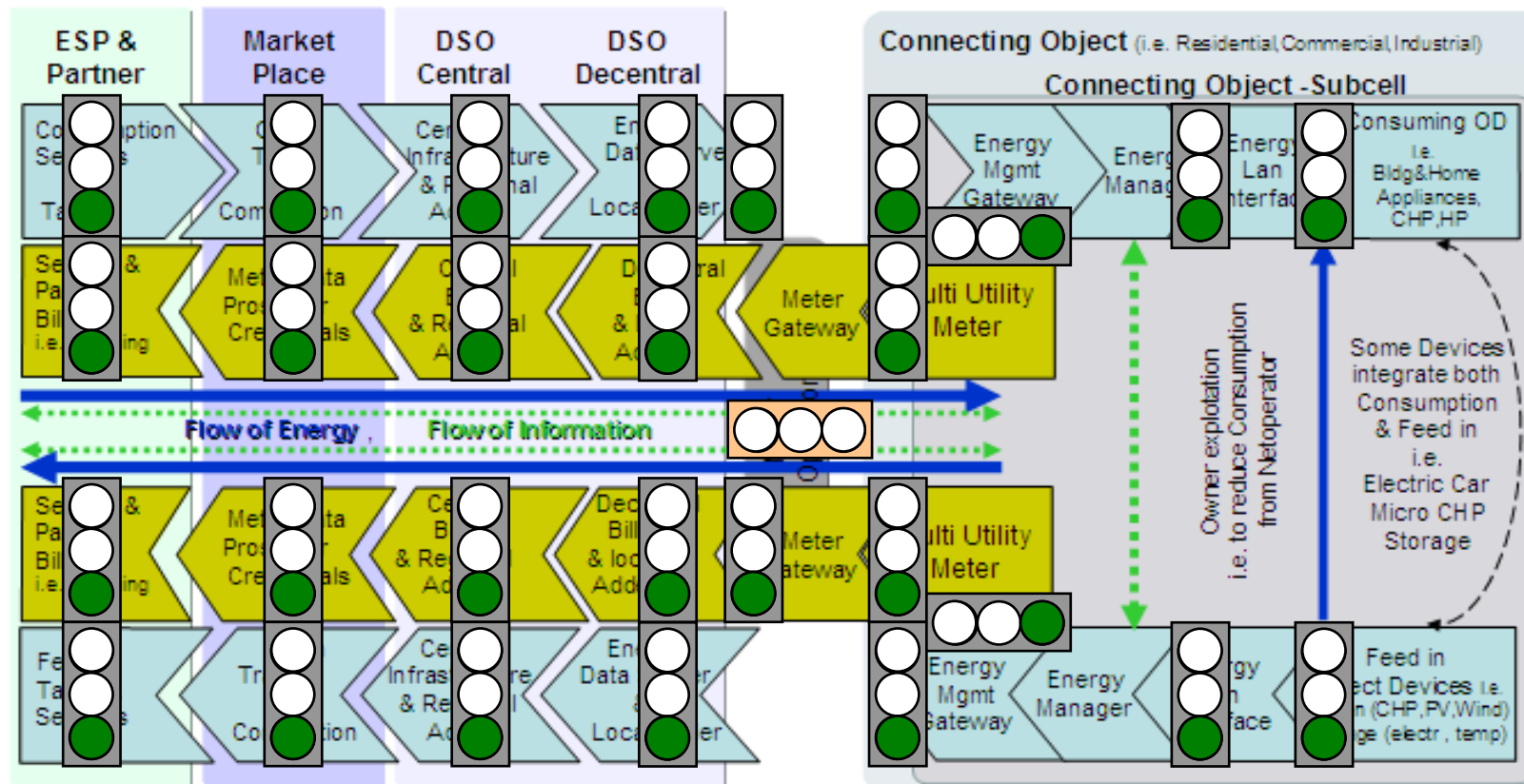
Informationssicherheit - Das Ziel



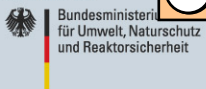
Gesamtsystem

DKE Kompetenzzentrum E-Energy Fokusgruppe Inhouse Automation

Smart Grid & Smart Meter Wirkungsdomänen



Gefördert durch das



Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit

Technisch

Organisatorisch

Danke für Ihre Aufmerksamkeit

Alfred Malina

Technische Unternehmensvertretung
IBM Deutschland MBS GmbH
Hechtsheimer Str 2
55131 Mainz



Telefon +49 6131 84 2419
Email malina@de.ibm.com

