TeleTrusT-interner Workshop 2011

München, 30.06./01.07.2011

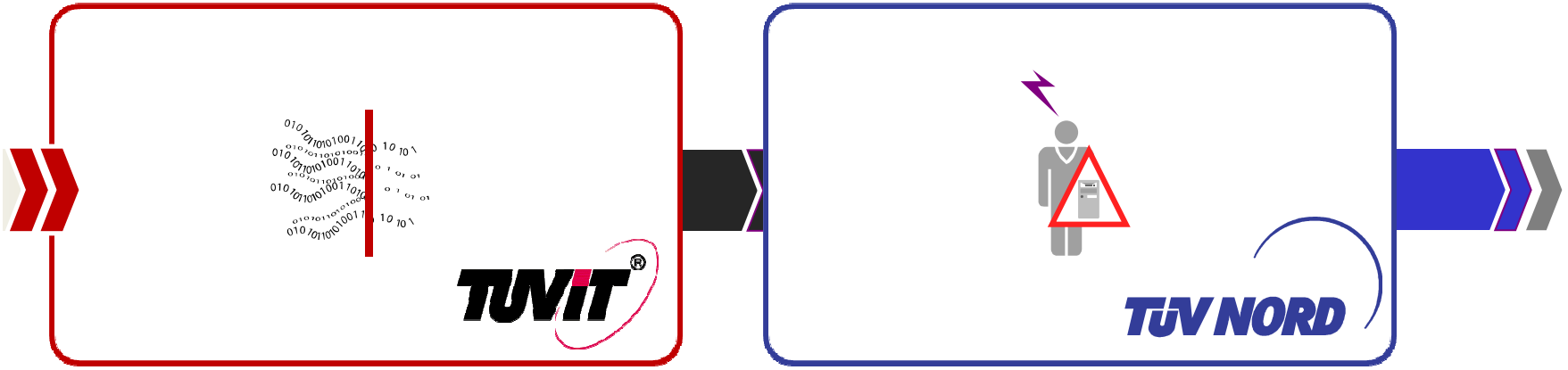
Markus Bartsch
TÜViT GmbH

IT Security im Smart Grid

IT Security und IT Safety

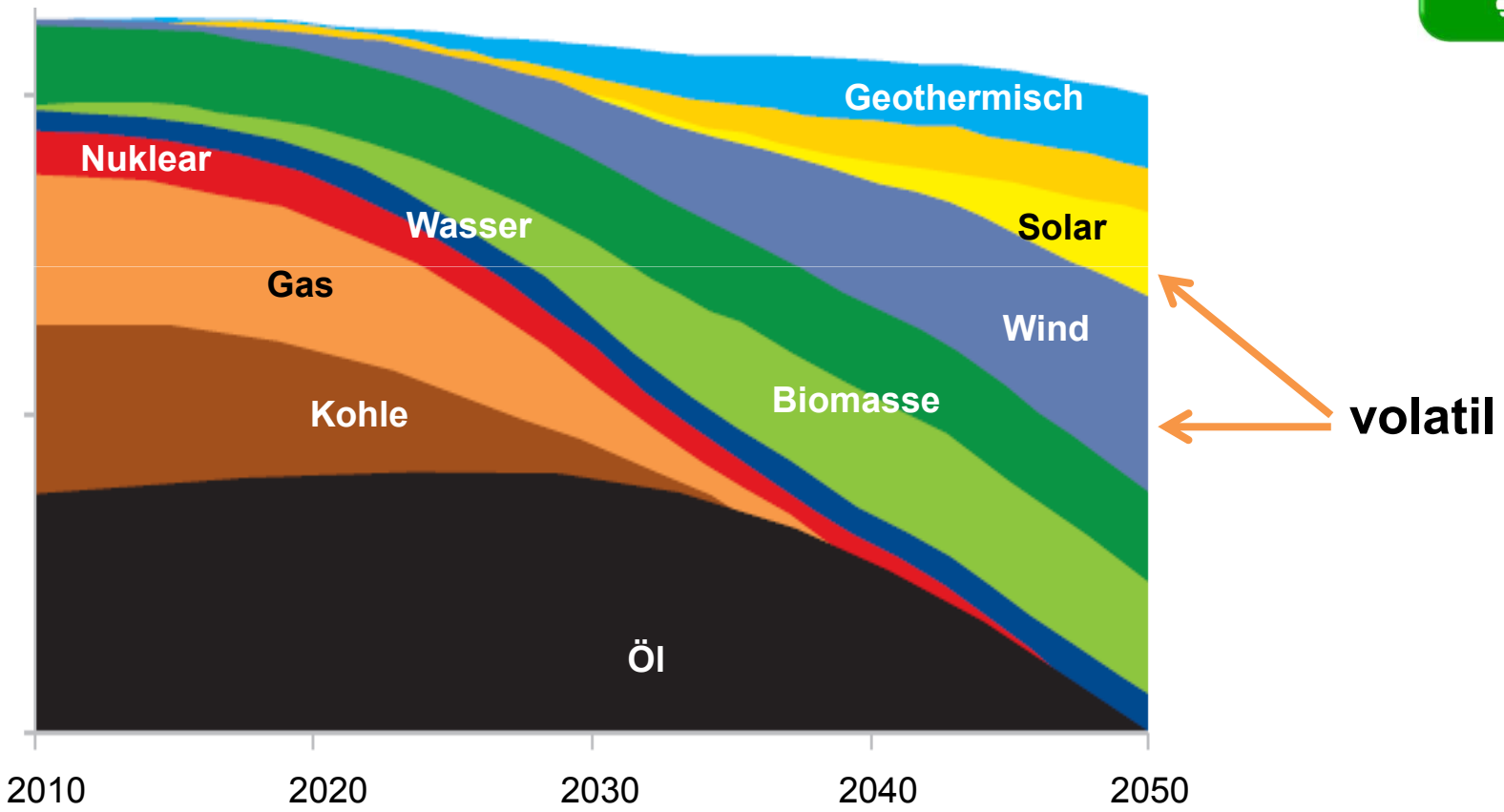
Security **SECURITY** Security

Safety **SAFETY** Safety



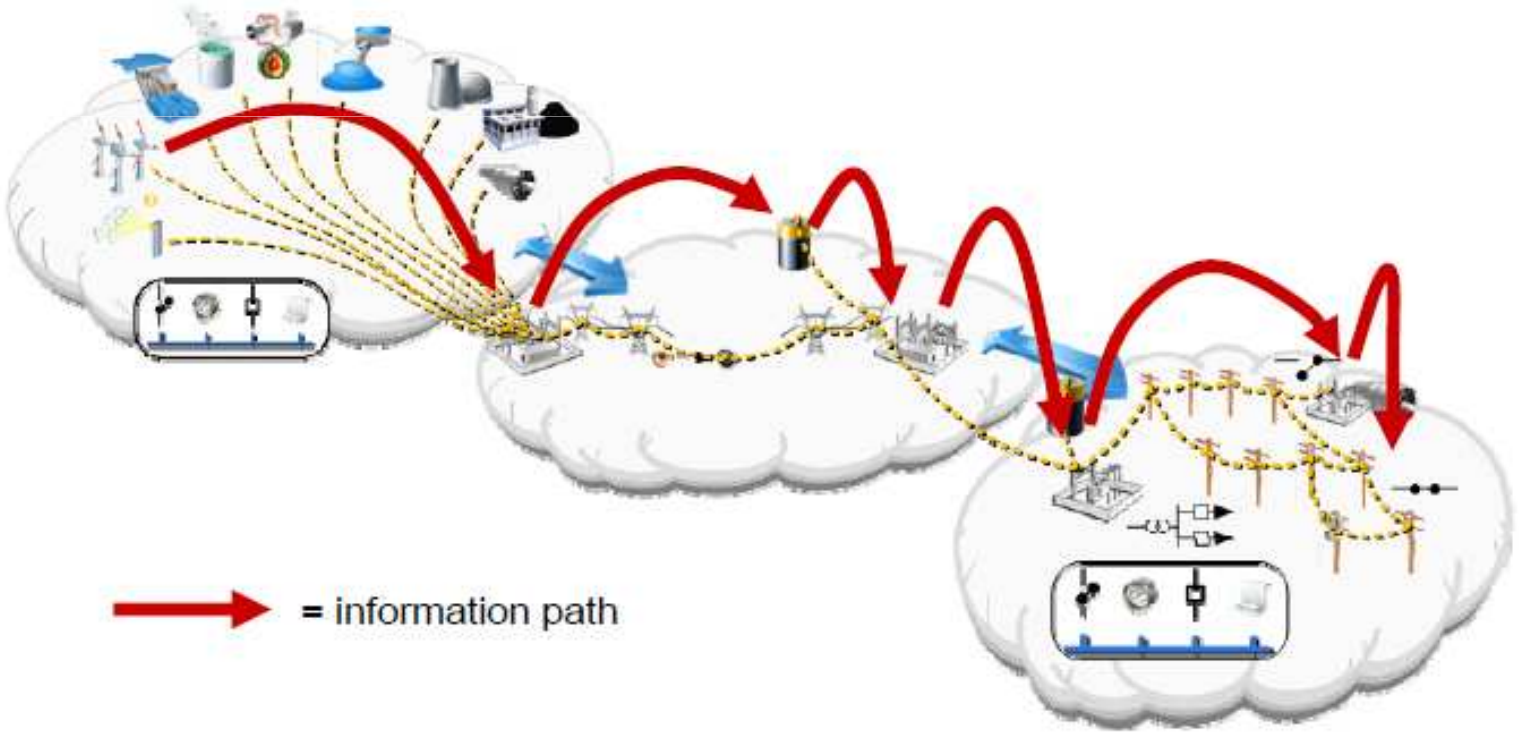
Threats
by man
→ Protection of **IT**

Zukünftige Energiequellen



Smart Energy – Metering und Grids
zukünftig: IKT ist wesentlicher Bestandteil

- Zentralisierte und verteilte **volatile** **Energieversorgung**
- **Lastmanagement** in Verteilnetzen
- Flexibles **Tarifierung**
- **Sichere** **Informationsverarbeitung** für Verbrauchs- und Steuerdaten



© Report to NIST on the Smart Grid Interoperability Standards Roadmap, 17.06.2009

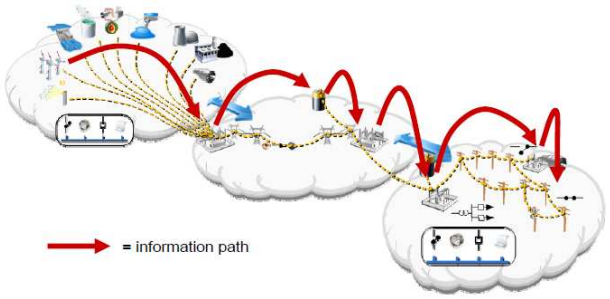
Smart Energy: Tomorrow (2020)

Organisation	Unterschiedliche Rollen, schnell wechselnde Partner
Demand Control	für Großabnehmer / Endkunden
Metering	vernetztes Smart Metering
IT-Systeme	komplett vernetzte IT Systeme
Pricing	Zeitabhängig, ggf. Nutzenabhängig
Renewables	> 20% (*~50%*) Grid Verhalten durch Renewables Virtuelle Kraftwerke
eMobility	großflächig ausgerollt, Anfänge von V2G

Politische Ziele in Deutschland
bis 2020

- 20% Anteil an erneuerbaren Energien
- 20% weniger Treibhausgasemissionen als 1990
- 20% mehr Energieeffizienz durch Verbrauchssteuerung

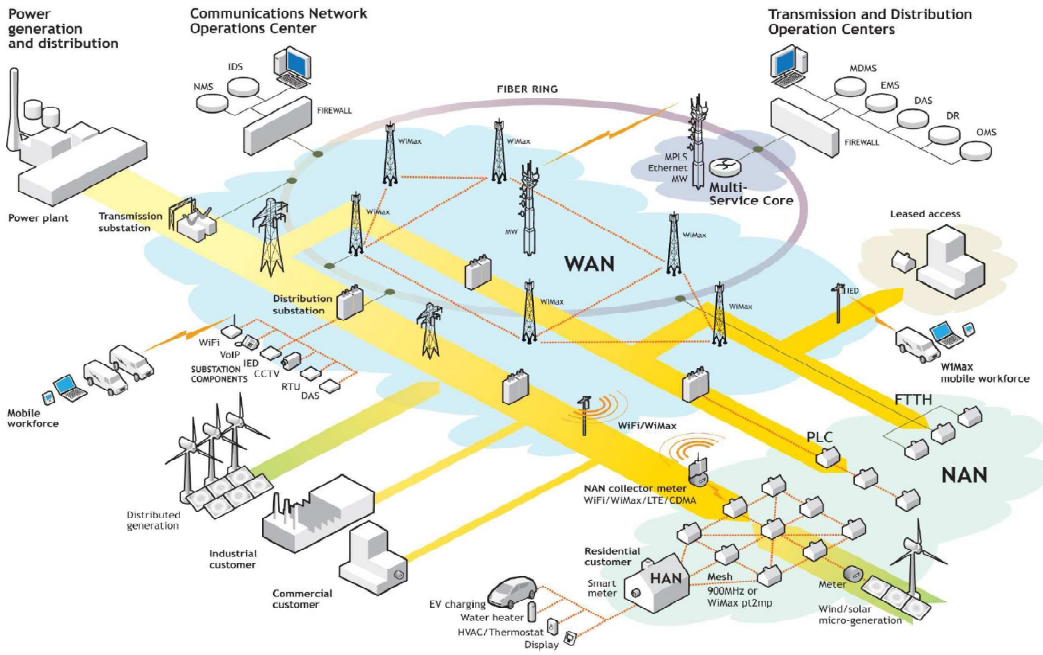
- Vorbereitung der **Elektromobilität**
  (2020: eine Million BEVs)
- Mehr **Wettbewerb** unter den Energieerzeugern und Verteilnetzbetreibern
- Aufbau einer **sicheren IT-Infrastruktur** zur Steuerung der Energienetze
  und ihrer Endeinrichtungen
- Gewährleistung von **Datenschutz** und **Datensicherheit** nach deutschem Standard
  mit gesetzlicher Verankerung



Smart Grid – Information und Kommunikation

Smart Meter / ICT Gateways

Maintenance



Managed Agents

Portale

eMobile Ladestationen

Kommunikation, z.B.
- **Netzwerk: RFID, LAN, WAN**
- **Web Services,...**

Problempunkte in der Prozessleittechnik
...und auch im Smart Grid

– Einzug der **klassischen IT** in die ursprünglich autark betriebene Prozessleittechnik:
  - Standardnetzwerk-Protokolle
  - Commercial Off The Shelf-Software
  - Anbindung an klassische IT
  - Anbindung an das Internet

→ **Bedrohungen aus der klassischen IT**

– Unterschiedliche **Anforderungen**

Klassische IT	**CIA**	**Prozessleittechnik**	**AIC**
Confidentiality	(**HOCH**)	Confidentiality	(**NIEDRIG**)
Integrity	(**MITTEL**)	Integrity	(**MITTEL**)
Availability	(**NIEDRIG**)	Availability	(**HOCH**)

→ **Klassische Sicherheitskonzepte nicht anwendbar**

IT Security
Gestern – Heute – Morgen

1983: Fred Cohens erster Computervirus

1988: „Morris Wurm“

1988: Baukasten für Viren

1991: erster polymorpher Virus

1998: „Telefonkarten-Hack“

2000: erster Trojaner für PDAs

2006: Phishing

2007: Skimming“

2010: “Underground Markets”

2010: *Stuxnet* – „Begin of Cyberwar“

...

1985: Orange Book

1987: Start von Pay TV (Teleclub)

1989: German Criteria

1991: europäische ITSEC

1991: D-Netz

1993: WWW mit *Mosaic*

1995: Electronic Purse

1998: Common Criteria

1998: HBCI (ZKA)

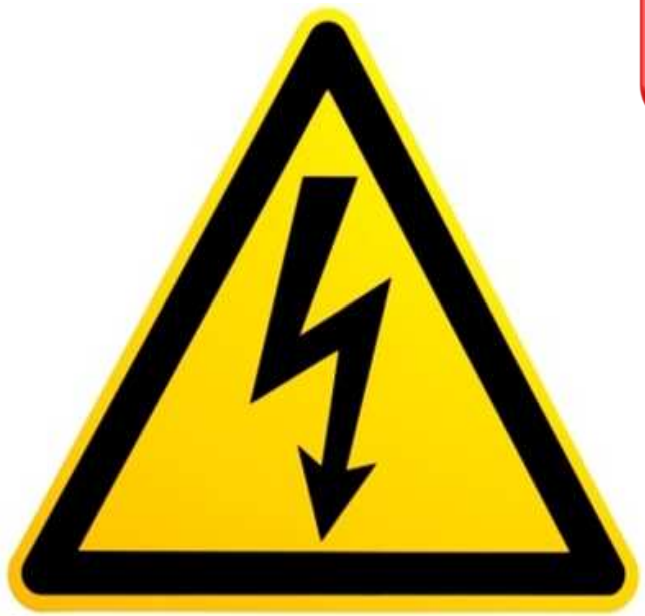
....

2010: nPA

2011: Security bei Smart Meter

Probleme im Smart Grid
Beispiele

- Datenschutz
- Betrug
- Cyber Crime

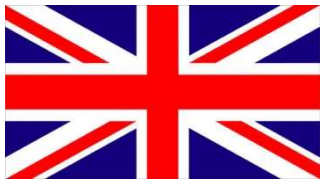


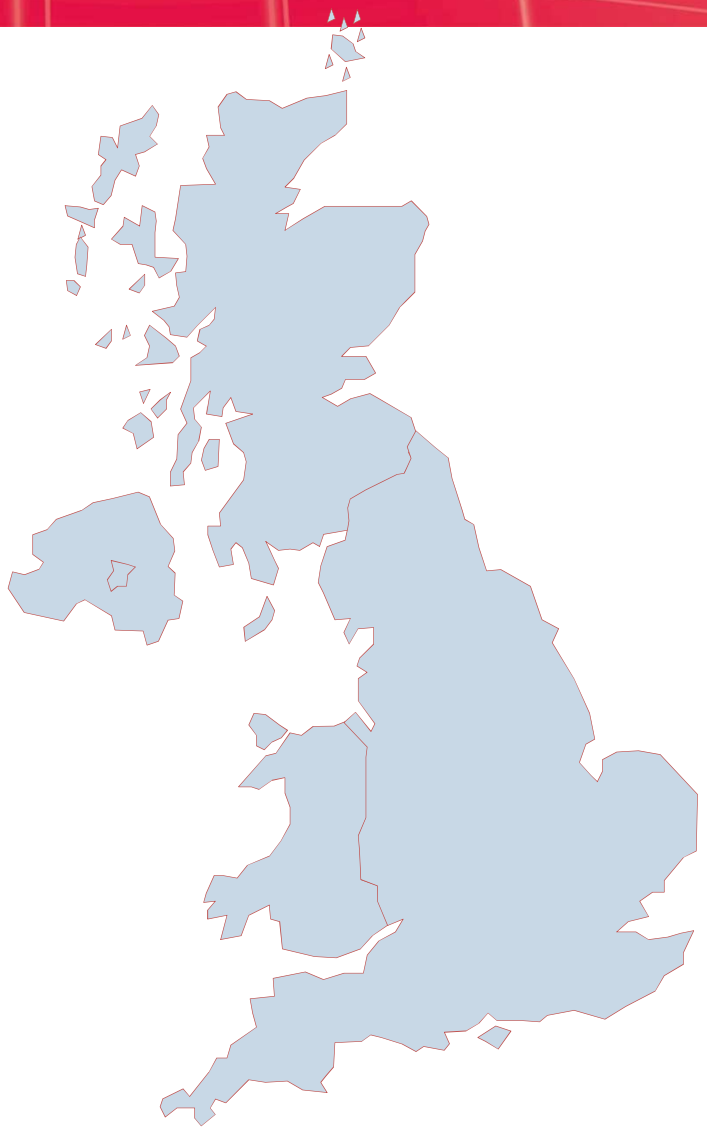
Beispiele (1)
Datenschutz

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

Beispiele (2)
Betrug: Prepaid Electricity Meter Fraud

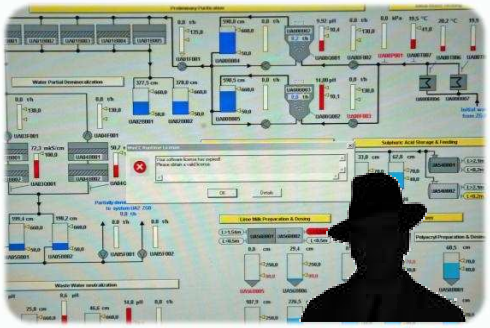




September 2010: Criminals across the UK have hacked the new key card system used to pop op pre-payment energy meters and are going door-to-door, dressed as power company workers, selling illegal credit at knock-down prices

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.

Beispiele (3)
Cyber Crime



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

Stuxnet

March 29, 2010

Smart Products | Smart Meters Vulnerable to Hack Attacks

By David Sims
TMCnet Contributing Editor

The new 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, 7:39am PDT | 2 Comments

Tweet 0 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 – Beginn des Cyberwar (1)

Gezielte Attacke gegen bestimmte IT Systeme

→ späte Entdeckung im Juli 2010 (Verteilung seit Juni 2009)

0-Day Exploits !!!

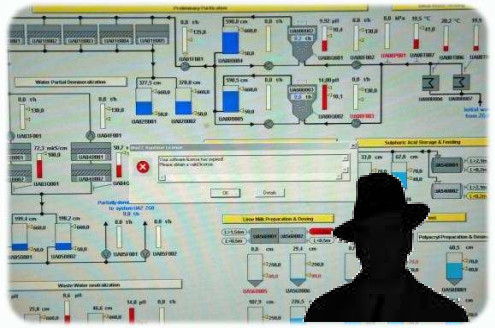
Tausende von Systemen waren infiziert!!!

06.2009 - First Distribution of Stuxnet

- 17.06.2010 - Virusblokada detects Stuxnet
- 16.07.2010 - Microsoft Security Advisory (.LNK-Exploit)
- 02.08.2010 - Patch 1. of 4 Exploit (.LNK)
- 14.09.2010 - Patch 2. of 4 Exploit (Print Spooler)
- 12.10.2010 - Patch 3. of 4 Exploit (Keyboard layout)
- 14.12.2010 - Patch 4. of 4 Exploit (Task-Scheduler)

Stuxnet – Beginn des Cyberwar (2)

- Charakterisierung
  - **Distributionsteil**: Computer Wurm
  - **Schadsoftware**:
    WinCC- und PCS7-Systeme mit bestimmter Konfiguration
  - **Auswirkungen**: Manipulation und Sabotage

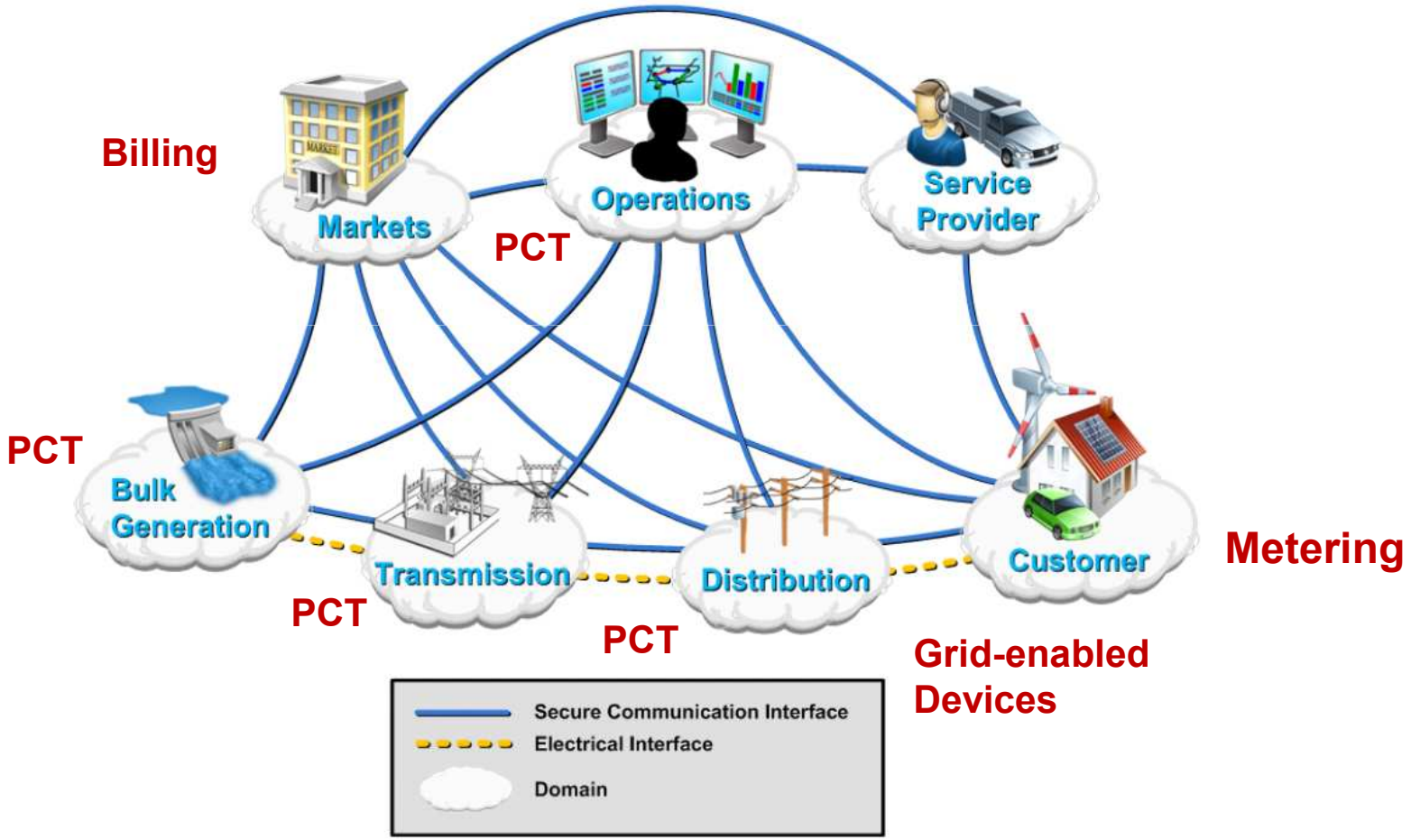


Source: http://www.freitag.de/community/blogs/sachichma/-stuxnet-der-suesse-hack

- Erstmals ist die Prozessleittechnik explizites Angriffsziel
  - Experten- und Insiderwissen
  - Einsatz spezieller Werkzeuge
  - hoher Resourcen- und Zeitaufwand

→ **HOHES Angriffspotential**

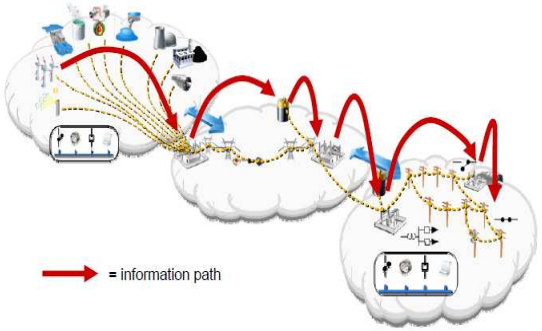
Smart Grid: Modell



Source: http://www.nist.gov/smartgrid/

Typische Security Funktionalitäten

- Identification / Authentication
- Authorisation
- Logging / Intrusion Detection
- Undeniable transfer of data (Signature)
- Trustworthy Channels
- Information Flow Control
- Redundancy in backend systems
- ...



„Kritische Infrastrukturen”

Sectors & Branches

Transport / Traffic
- Aviation
- Maritime traffic
- Rail traffic
- Road traffic

Energy
- Electricity
- Nuclear power
- Gas
- Oil

Production
- Chemical
- Biologic
- Pharmaceutics
- Defence

IT & T
- Telecom
- IT

Finance / Insurance
- Bank
- Insurance
- Stock exchange
- Clearing center

Supply
- Health care
- Rescue service
- Civil protection
- Food & Water
- Disposal

Government
- Federal Gov.
- State Gov.
- Municipalities
- Defense
- Police

Misc.
- Media
- R&D
- Culture goods & buildings

„Kritische Infrastrukturen”
bezüglich: Leittechnik

Sectors & Branches

Transport / Traffic	Energy	Production	IT & T
Aviation	Electricity	Chemical	Telecom
Maritime traffic	Nuclear power	Biologic	IT
Rail traffic	Gas	Pharmaceutics	
Road traffic	Oil	Defence	

Finance / Insurance	Supply	Government	Misc.
Bank	Health care	Federal Gov.	Media
Insurance	Rescue service	State Gov.	R&D
Stock exchange	Civil protection	Municipalities	Culture goods & buildings
Clearing center	Food & Water	Defense	
	Disposal	Police	

IT Security: Standards und Testmethoden

Sectors & Branches

Transport / Traffic
ISO 2700x
IT-Grundschutz
Common Criteria

Energy
VGB R 175
BDEW White Paper
(ISO 2700x)
IEC 62351
NISTIR 76258
WIB M2784-X-10
…

Production
ISA 99
IEC 62443
Namur NA115
…

IT & T
ISO 2700x
ITSEC
Common Criteria (ISO 15408)
FIPS 140-2
…

Finance / Insurance
ZKA
EMVCo
PCI
…

Supply
IT-Grundschutz

Government
IT-Grundschutz
ISO 27001
Common Criteria
FIPS 140-2

Misc.
?

Cyber Security – Normen und Standards

- „nur“ Empfehlungen oder **Best Practice**
  → *muss, soll, kann*
- **Vielfalt** an Material – nicht harmonisiert
  → *ISO/IEC JTC 1 / **SC 27***
- **Rollen** (*Betreiber, Vendor*) nur teilweise unterschieden
- **Priorisierung/Skalierung**
  (*Sicherheitslevel, Beschreibungstiefe*) nicht definiert
- keine konkreten **Schwachstellenanalysen** definiert
- **Prüfschema** fehlt
  → *Vergleichbarkeit*
- **Synergie** zwischen Security und Safety fehlt
  → *Threats vs. Hazards*

Schutz durch „Best Practices“

- Best Practices in Process Control Systems
  - Industrial Automation and Control Systems Security - ISA99 (ISA)
  - Cyber Security Procurement Language (DHS)
  - Critical Infrastructure Protection (NERC)
  - Guide to ICS Security (NIST - SP 800-82)
  - VGB R 175
  - …

- Practical Examples
  - Quarantine PC: Scan of USB sticks
  - Patch Management: Prioritization of Patches
  - Incident Response: defined Process
  - Data Flow Control: Segmentation (FW)
  - …

but:

concrete standards and evaluation methods do not exist and are not harmonized

Layers of Process Control Technology
- special Security Topics -

1. Field Instrumentation
   Field Bus, Actors, Sensors
2. **Process Control**
   BuB, Engineering, Online-Optimization and Diagnostic
3. **Supervisory Control / Process Control Access Domain**
   Logging and Control
4. Business Unit IT
   Data Management
5. Office IT
   Email, Data Server, Office IT
6. External DMZ / Internet

IT Security Funktionalitäten

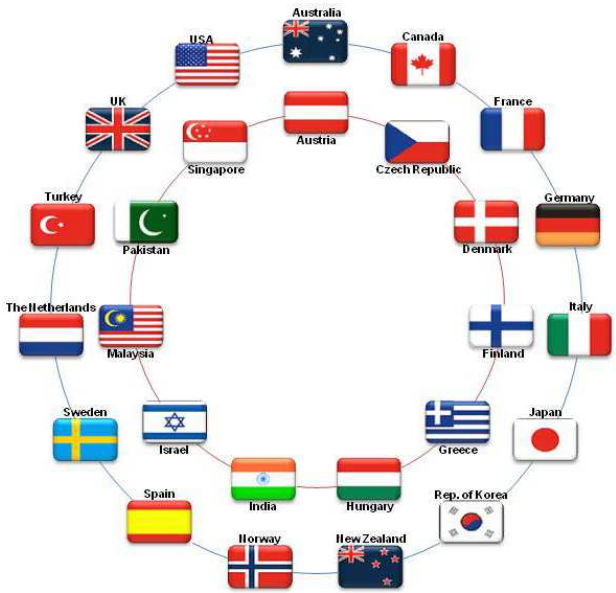
wurden für **Smart Meter Systeme** von **TÜViT**

und dem **BSI** spezifiziert - zusammen mit:

- BMWi
- BNetzA
- PTB
- BfDI

- *Schutzprofile (Protection Profiles)* nach den internationalen

Common Criteria



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

Europäische Anerkennungsvereinbarung
(SOGIS-) MRA

- Anerkennung von Common Criteria und ITSEC Zertifikaten
- Schließt alle Evaluationsstufen von EAL1 bis EAL7 ein (je nach "Technical Domain")

Smart Meter:
IT Security und Datenschutzanforderungen

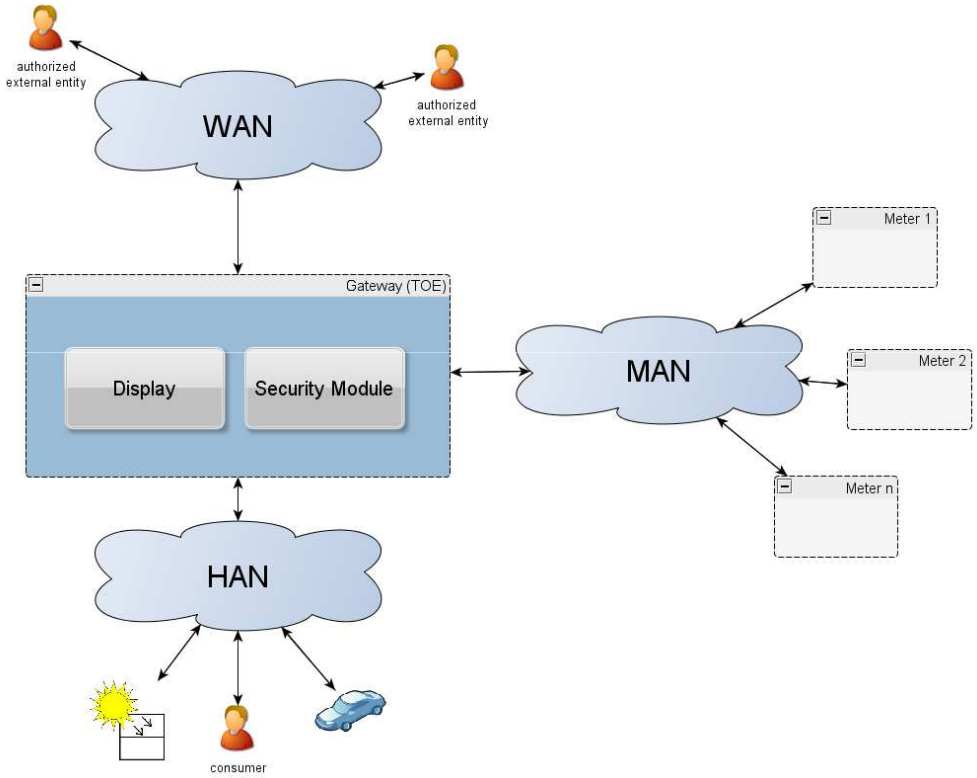
Bundesamt für Sicherheit in der Informationstechnik

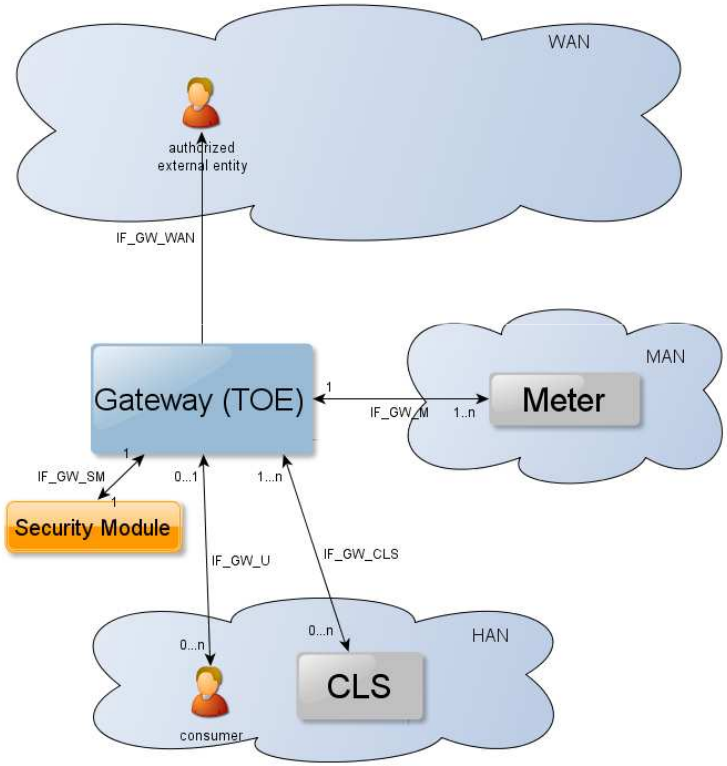
TÜViT®

- **Verfügbarkeit, Integrität** und **Vertraulichkeit** der an die Messstellendienstleister übermittelten **Verbrauchs-** und **Einspeisedaten**
- **Gewährleistung der Versorgungssicherheit**
  Ausschluss negativer Rückwirkung vereinzelter oder massenhafter Fehlfunktionen wie auch gezielter Manipulationen von Smart Metern auf die Versorgungssicherheit
- **Manipulationssicherer Betrieb der Smart Meter**
  in ungesicherter Umgebung (Hausflur)
- **Datenschutzanforderungen**
  Verhinderung der Erstellung und Weitergabe von Verbraucherprofilen gemäß gesetzl. Vorgaben / Einstellungen des Kunden
- **Steuerung der Zugriffskontrolle je nach Rolle**
  der Marktteilnehmer, z. B.: Verbraucher, Netzbetreiber, Stromlieferant

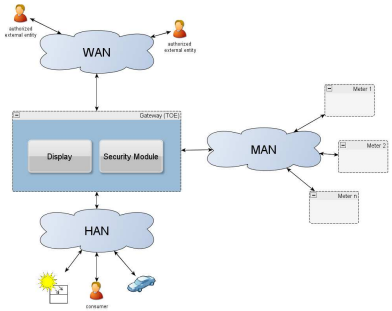
IT Security für Smart Meter (1)

Smart Meter Gateway - Architektur





Special Security Features
Smart Meter Gateway

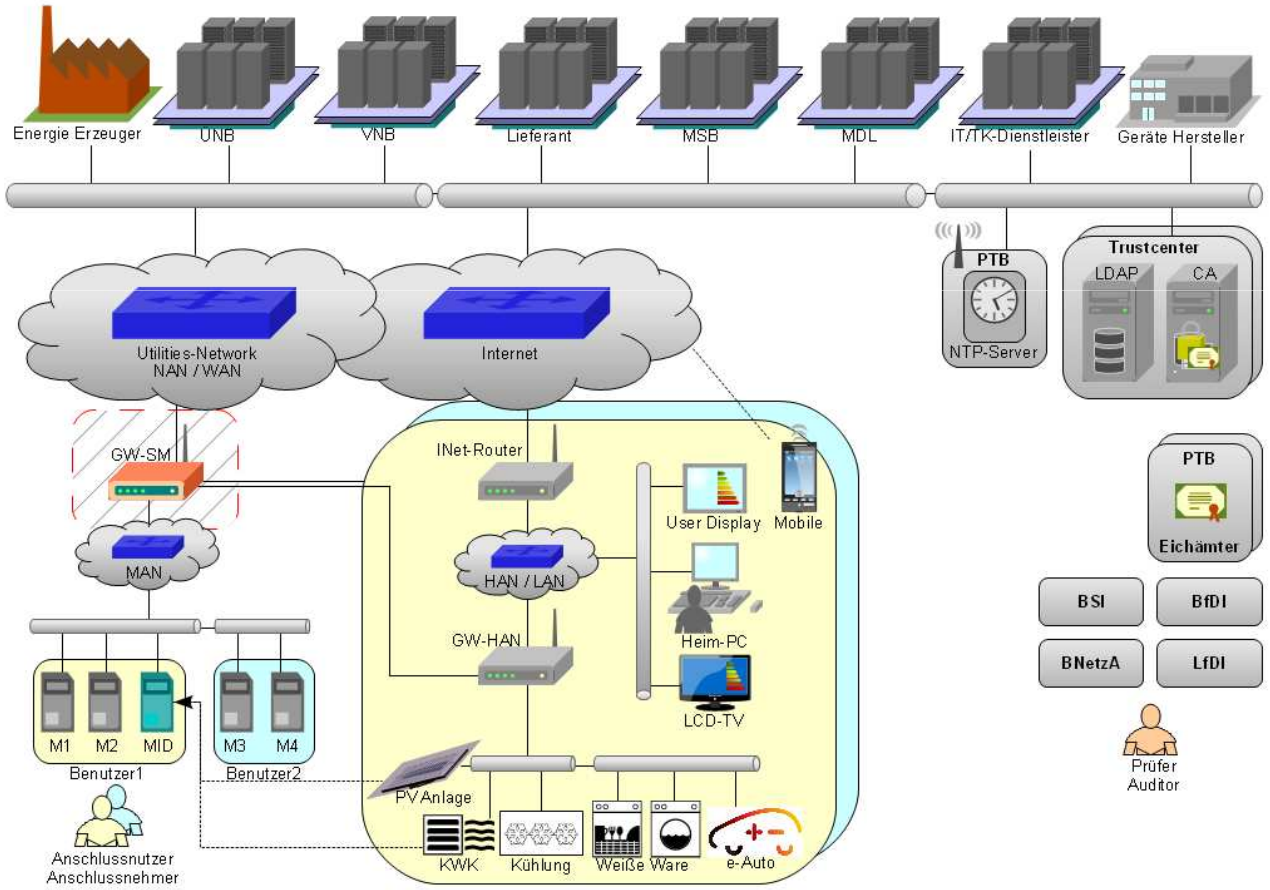


- Logging (**O.Log**)
- Cryptography /
  Trustworthy Channels (**O.Crypt**)
- Information Flow Control (**O.Firewall, O.SeparateIF**)
- Secure Handling of meter data (**O.Meter**)
- Protection of Security Functions (**O.Protect**)
- Concealment (**O.Conceal**)

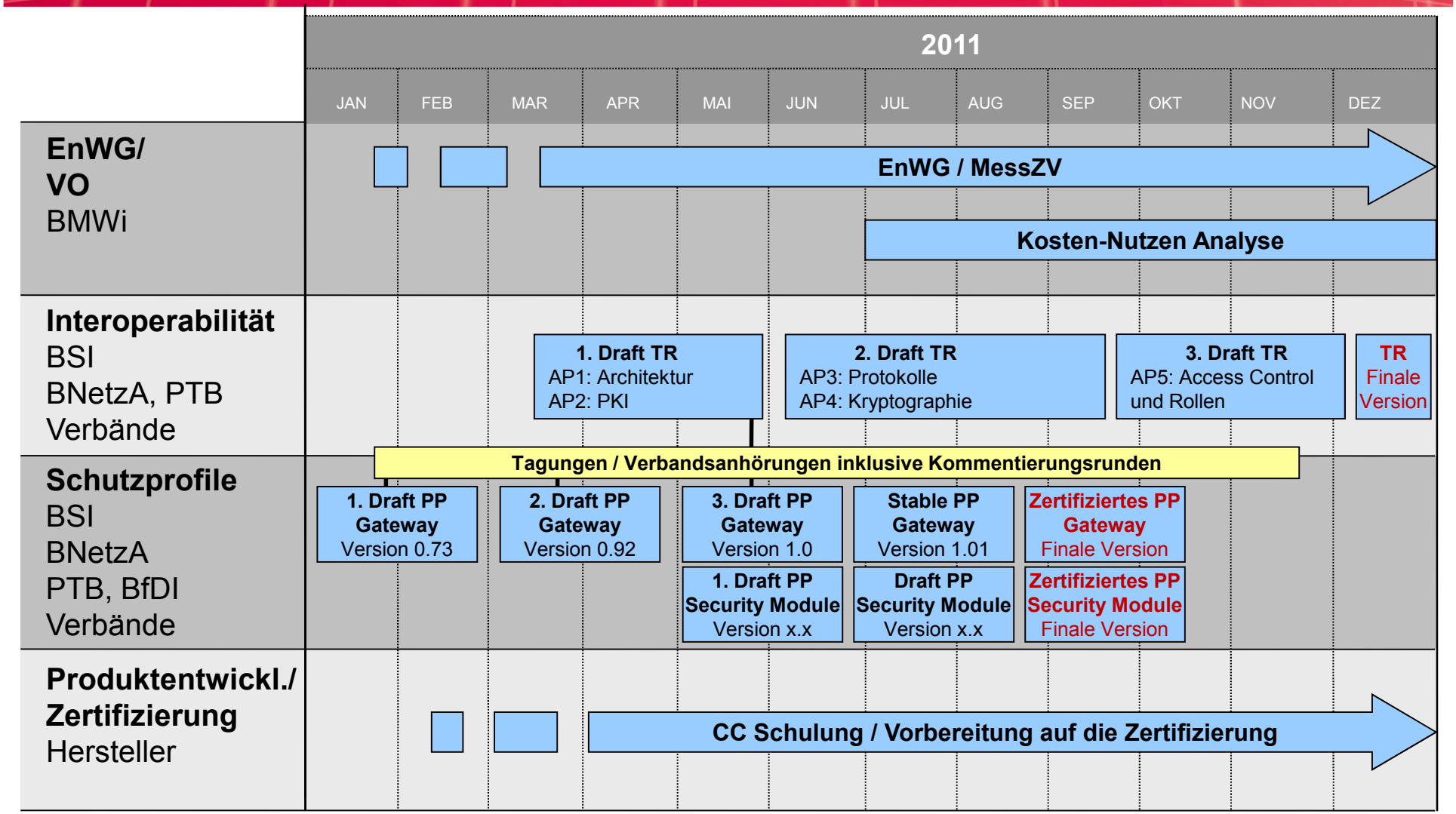
IT Security für Smart Meter (2)

Technische Richtlinien: geplante Systemarchitektur

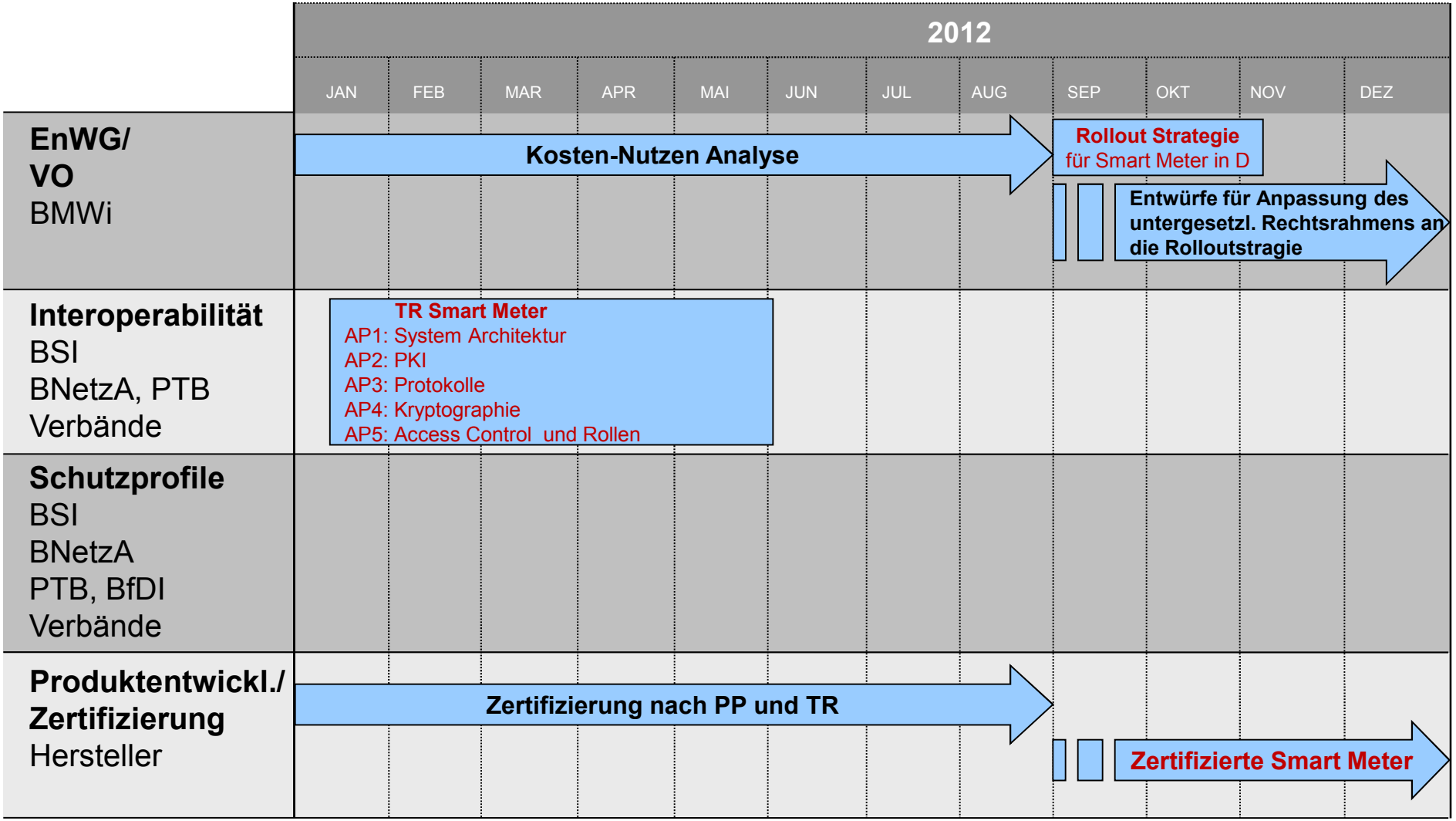
- PKI
- Kommunikations-protokolle
- Kryptographie
- Zugriffskontrolle



Roadmap Smart Meter (2011)



Roadmap Smart Meter (2012)



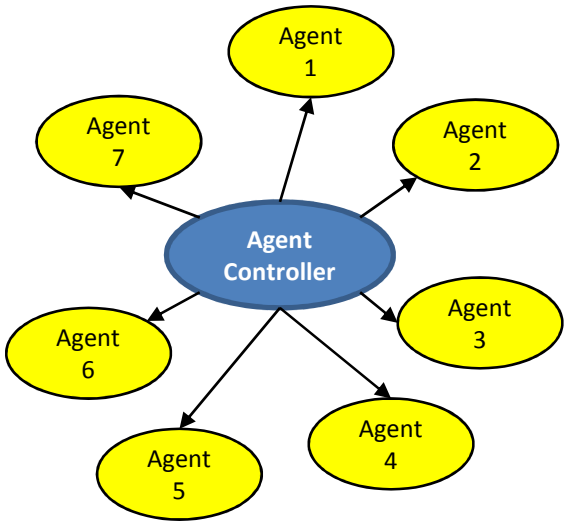
MAS – Multi Agenten Systeme (1)

Multi-Agenten-Systeme (MAS) sind Systeme, in denen mehrere Agenten mit definiertem Funktionsumfang eigenständig oder zentral koordiniert miteinander arbeiten:

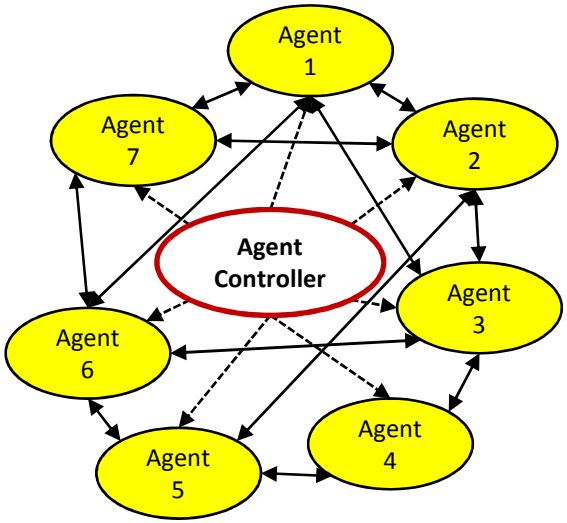
- **Autonomous:** eigene Entscheidungen
- **Proactive**: Actionen ohne äußeren Impuls
- **Reactive**: Actionen aufgrund eines äußeren Impulses
- **Interactive**: Koordination des Betriebs

MAS – Multi Agenten Systeme (2)

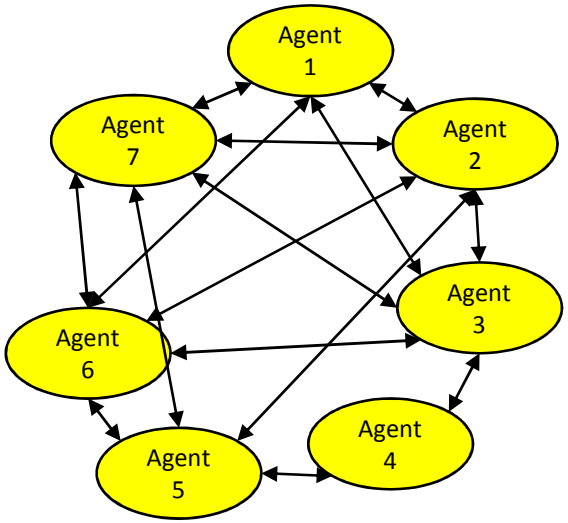
Zentrale Steuerung



Verteilte Steuerung



Peer-to-Peer



MAS – MAS – Multi Agenten Systeme (3)
Voraussetzungen

- Entwicklung intelligenter, (teil-) autonomer Softwarekomponenten
- Definition einheitlicher und sicherer Kommunikationsstandards (*IEC 61850*)
- großflächiger Einsatz zusätzlicher Sensoren und Aktoren:
  - für die Informationsversorgung der Agenten und
  - für steuernde Eingriffe durch die Agenten
- Implementierung von IT Security Funktionalitäten *(siehe: Smart Meter GW)*
- → Management der IT Security Funktionalitäten
  - Geräte-PKI
  - Authorisierung der Geräte
  - Rollenkonzept
  - …

Vendor:
Beispiele für IT-Sicherheitsanforderungen

- **Anwendung**
  - Account Management
  - sichere Webanwendungen
  - Integritätschecks relevanter Daten
- **Systemhärtung**
  - Entfernen von nicht benötigten Diensten und Programmen
  - Host Intrusion Detection
- **Malicious Code**
  - Virenentdeckung
  - Prozesse zur Entfernung
- **Patch Management**
  - Patches für die COTS-Produkte
  - Behandlung von Sicherheitsvorfällen
  - Sichere Updateprozesse
- **Fernzugriffe**
  - Fernwartung
  - Modems
  - Authentisierung und Autorisierung

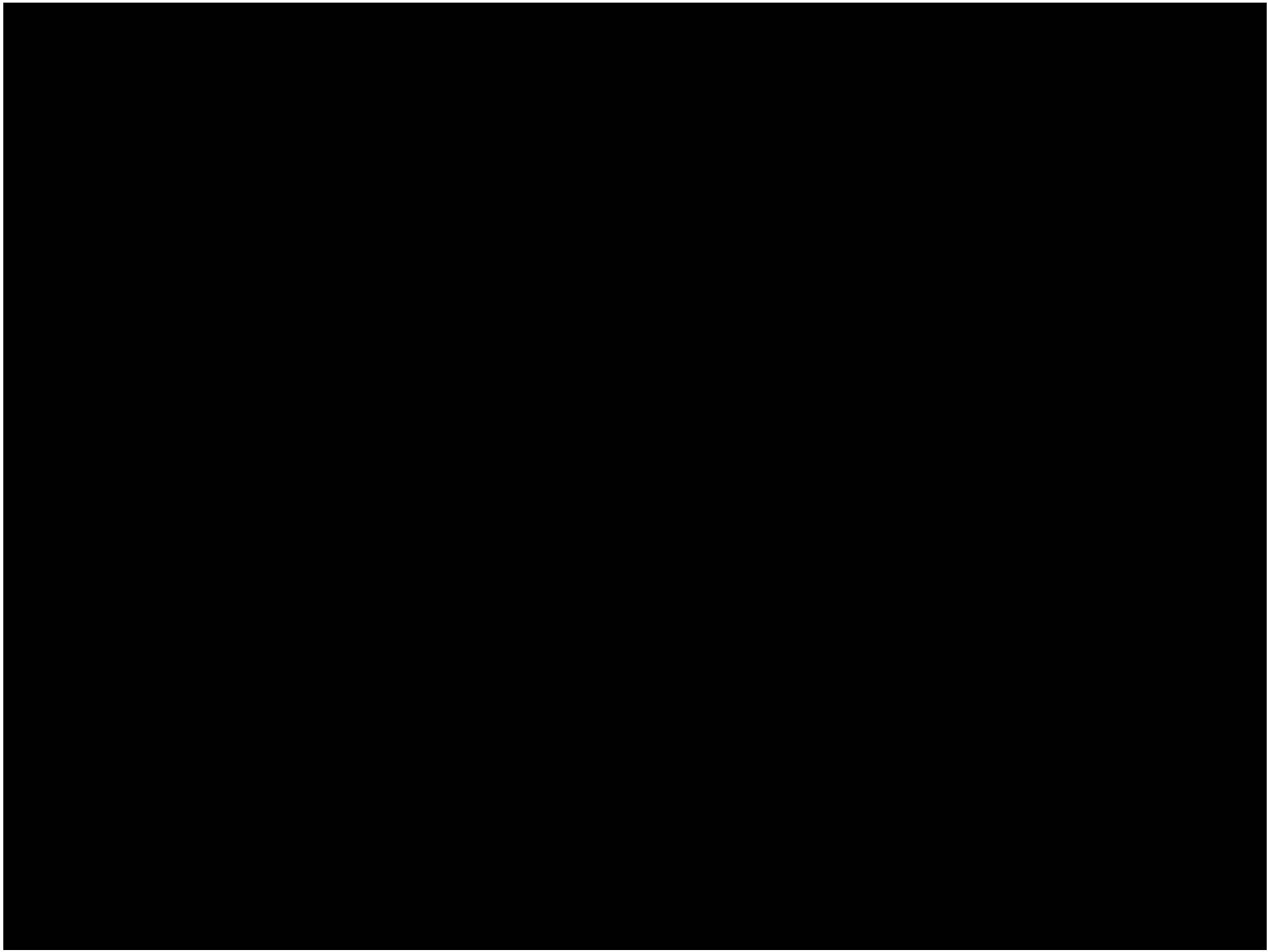
Betrieb:
Beispiele für IT-Sicherheitsanforderungen

- **Physikalische Absicherung**
  - Endgeräte
  - Zutritt zur Leitstelle
  - Zugang zu den Netzwerken und Systemen
  - Schlüsselvergabe und –verwaltung
- **Absicherung des Perimeters**
  - Netzwerkarchitektur
  - Verbindungen in die Leittechnik
  - Firewalls
  - Netzwerksegmentierung
  - Funktechnologien
- **Prozessschnittstelle und Endgeräte**
  - Plausibilitätschecks der Werte
  - Datenübertragung
  - Intelligent Electronic Devices
  - Remote Terminal Units
  - Programmable Logic Controllers
  - Sensoren und Messsysteme
- **Datensicherung**, -wiederherstellung und Notfallplanung

IT Security für Smart Grids: ToDo

- **IT Security Management**
- **Nutzen von IT Security Technologien**
  - **Nutzen der IT Security Industrie**
- **Standardisierung der IT Leittechnik**

Harmonisierung von Cyber Security
Hersteller sollten sich auf **einen** **Standard** konzentrieren
(*international* und *branchenübergreifend*)



IT Security im Smart Grid

Lösungen der IT Security Industrie

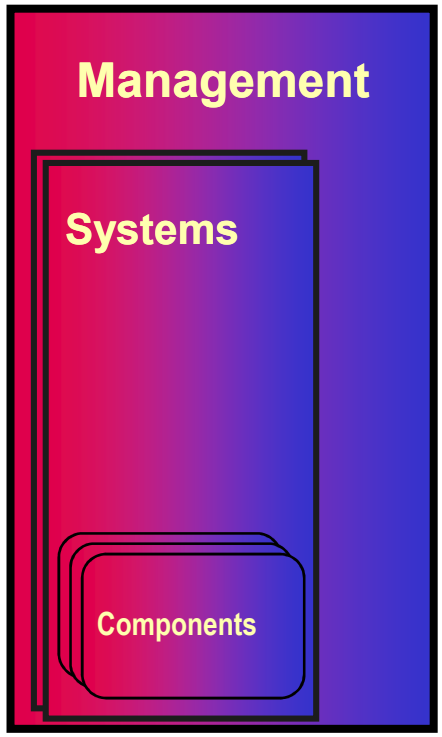
Vertrauen durch IT Security Evaluationen / Audits

ISO 27001

Energy

VGB R 175
BDEW White Paper
(ISO 2700x)
IEC 62351
NISTIR 76258
WIB M2784-X-10
…

Common Criteria



- **Security Policy**
- **Security Management**
- **Security Concepts**
- **Training**

- **Transfer Networks**
- **Distribution Networks**
- **Public Key Infrastructures**
- **Backend Systems**
- **Data Centers**
- **Charging Infrastructure (BEV)**
- **Billing Systems**
- **SCADA / PCT**
- **Smart Home**

- **Industrial Security Components**
- **FE Applications**
- **Gateways**
- **Smart Cards**

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