TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Smart Grid„

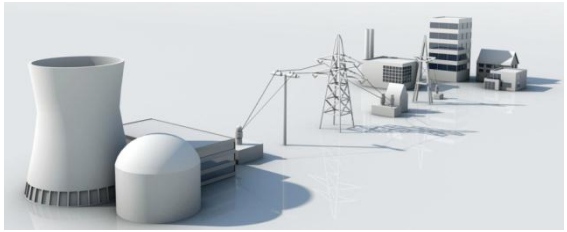
Berlin, 13.06.2013

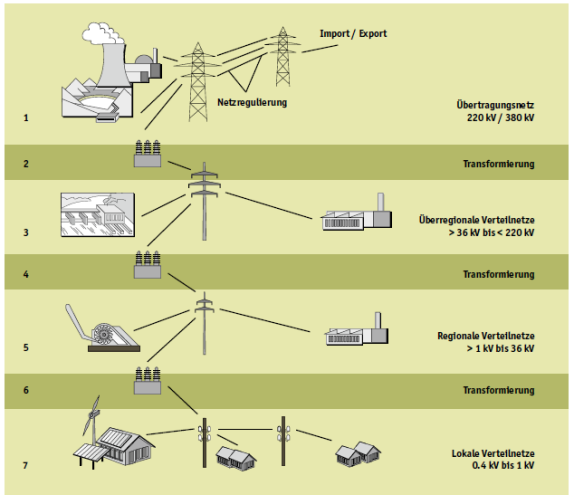
Sicherheitsaspekte im Smart Grid aus Schweizer Sicht

Christian Meier, Landis+Gyr

Was ist ein Smart Grid

Wie sahen Energienetze aus bis fast heute





Quelle: VSE / Die Volkswirtschaft

- Zentrale Erzeugung in Kraftwerken (Gas-, Kern-, Wasser-,…)
- Grossflächige Verteilung über 220/380kV Netz
- Überregionale Verteilung im 36kV bis 220kV Netz
- Regional Verteilung im 1kV bis 36kV Netz
- Lokale Verteilung im 400V bis 1kV Netz

Was ist ein Smart Grid

Energie Netze Morgen -> das Smart Grid

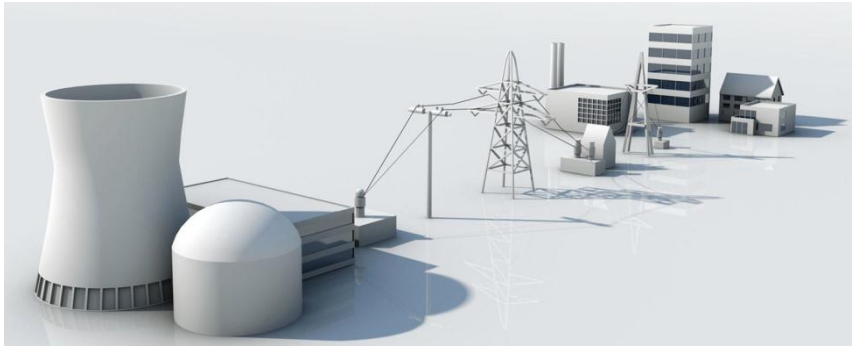
- Weiterhin Einspeisung aus Kraftwerken
- Verteilung der Energie weiterhin über Verteilnetze (Überregional, Regional, Lokal)
- Massive Zunahme an Einspeisung im lokalen Verteilnetz
- Veränderte Verbrauchskurven (Smart Home)
- Rückwirkung der Einspeisung auf Verteilnetze
- Dynamisches Lastmanagement
- Dynamisches Einspeisemanagement
- Dezentrale Erzeugung, Bilanzierung und Verbrauch
- Zentrales Netzmanagement
- Einbindung Kommunikativer Netzknoten
- Intelligente Knoten mit Autonomie

Anforderungen und Motivatoren zu Smart Grid Security

- EU Energie Effizienz Direktive mit Mandat zum Roll out von Smart Metern bis 2020
- Energiewende durch abschalten von AKWs -> Smart Grid wird absolut essentiell
- Datenschutz ist ein hoch einzustufendes Grundrecht und gesetzlich stark verankert
- Nichtbeachten von diesem Grundrecht kann schwerwiegende Folgen haben für Staaten und Unternehmen
- Smart Metering ist die erste Phase Richtung IKT vernetztem Smart Grid
- Zukünftige Angriffe verlagern sich immer mehr in den Cyber Space
- Energie Netze sind volkswirtschaftlich relevante Infrastrukturen und müssen daher angemessen geschützt werden

Anforderungen an IT Security

Auf Stufe Produzenten und Übertragungsnetzbetreiber…



- **Peripherie Sicherheits-Konzepte**
- **Gesichter Übertragungskanäle (Physikalisch und mit TLS)**
- **Gesicherte Umgebung (Nur Unternehmenseigene «Gebäude»)**
- **Gesicherter Zugang**
- **Office Security**
  - Firewalls
  - Patch Management
  - Intrusion Detection Systeme
  - Virenschutz
- **Zertifizierung (nach ISO 27002 (-9))**

Anforderungen an IT Security

Auf Stufe Verteilnetzbetreiber und Lieferanten

- **Datenschutz**
  - Zugangsschutz
  - Inhaltsdaten Verschlüsselung CMS
  - Datensparsamkeit
  - Digital signierte Werte
- **Sicherheit**
  - Integrität zwecks Netzsteuerung
  - Verfügbarkeit zwecks Netzsteuerung und Abrechnung
  - Sicherer Schlüsselaustausch
  - Reaktionsfähigkeit im Falle von kompromittierten Netzen
  - Sichere Übertragungskanäle
  - Zertifizierte Hersteller
  - Zertifizierte Anwender

Situation Schweiz

Status Umsetzung Anforderungen

- **Peripherie Sicherheits-Konzepte**
- **Gesichter Übertragungskanäle (Physikalisch und mit TLS)**
- **Gesicherte Umgebung (Nur Unternehmenseigene «Gebäude»)**
- **Gesicherter Zugang**
- **Office Security**
  - Firewalls
  - Patch Management
  - Intrusion Detection Systeme
  - Virenschutz
- **Zertifizierung (nach ISO 27002 (-9))**

- **Datenschutz**
  - Zugangsschutz
  - Inhaltsdaten Verschlüsselung CMS
  - Datensparsamkeit
  - Digital signierte Werte
- **Sicherheit**
  - Integrität zwecks Netzsteuerung
  - Verfügbarkeit zwecks Netzsteuerung und Abrechnung
  - Sicherer Schlüsselaustausch
  - Reaktionsfähigkeit im Falle von kompromittierten Netzen
  - Sichere Übertragungskanäle
  - Zertifizierte Hersteller
  - Zertifizierte Anwender

Situation Schweiz - Rechtliche Rahmenbedingung

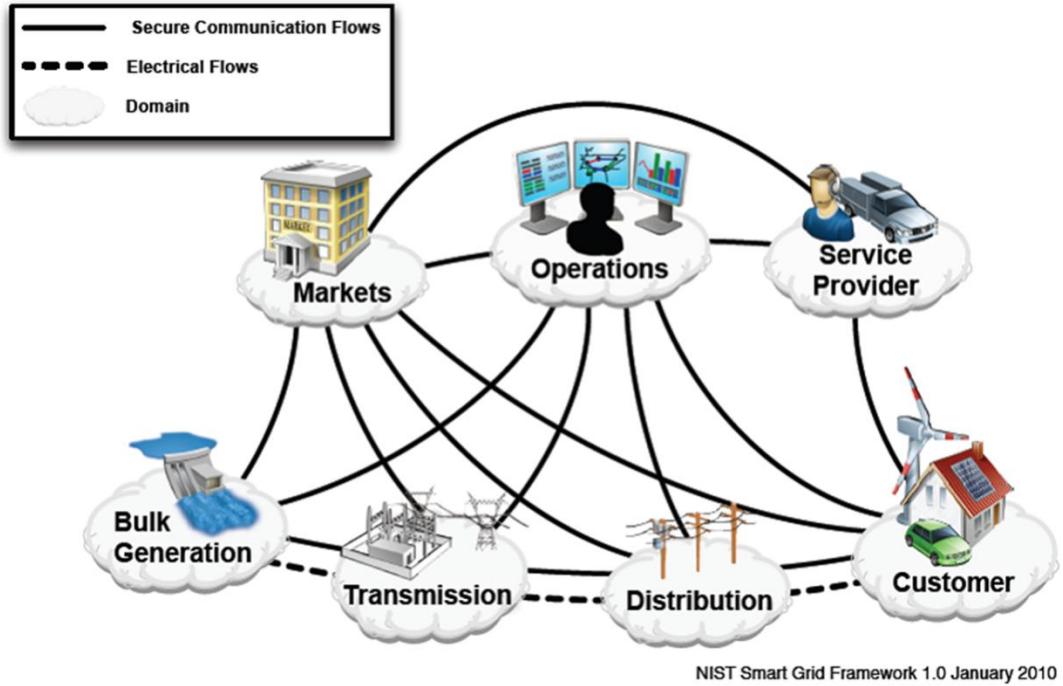
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Energie BFE

- **Bundesamt für Energie hat ein Bericht vorgelegt, in Zusammenarbeit mit Elektrizitätswerk der Stadt Zürich, Author Martin Loher, Compass Security**
- **Bericht IT Sicherheit bei Smart Metering**
  - Auf Verschiedene Architekturen bezogene Analyse: Gateway bassierte Smart Meters, Netzwerk/Firewalling, Server hardening,PLC basierende Smartmeters
- **Bericht ist verglichen mit Regulatorischen Anforderungen in anderen Ländern sehr vage und stellt keine konkreten Anforderungen**
- **In der Schweiz wird es darauf hinaus laufen, dass die EVUs und die Hersteller selbst die IT Security Konzepte spezifizieren müssen -> Gefahr eines Flickenteppichs**

Situation Schweiz

Grundlegende Ansätze:



NIST Smart Grid Framework 1.0 January 2010

Situation Schweiz

Basis DLMS/COSEM und NISTIR 7628

DRAFT NISTIR 7628

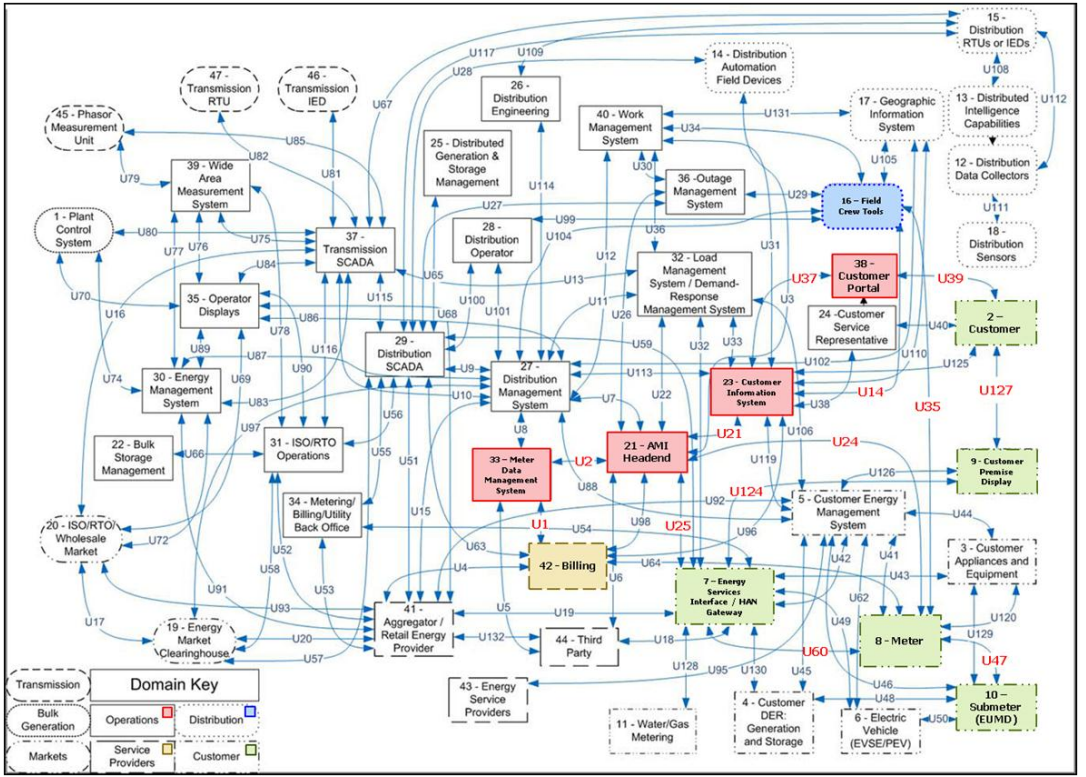
Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy

The Smart Grid Interoperability Panel–Cyber Security Working Group

July 2010

U. S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director



Smart Grid Security

Was ist im Einsatz:

- **Zugangs-Authentifizierung (Client & Server)**
- **Verschlüsselung und Signierung von Inhaltsdaten auf Applikation-Ebene**
  - Symmetrische Verschlüsselung AES-GCM-128
  - Asymmetrische Verschlüsselungen mit ECC und RSA Algorithmen
- **TLS Kanal Verschlüsselungen vor allem in WAN Kommunikation**
- **PKI mit staatlichen Root CA**
- **W3C Sicherheitsstandards**
- **Common Criteria Zertifizierung (für Deutschland)**
- **NISTIR als Rahmenwerk für E2E Sicherheitskonzepte**

Situation Schweiz

Wohin geht es

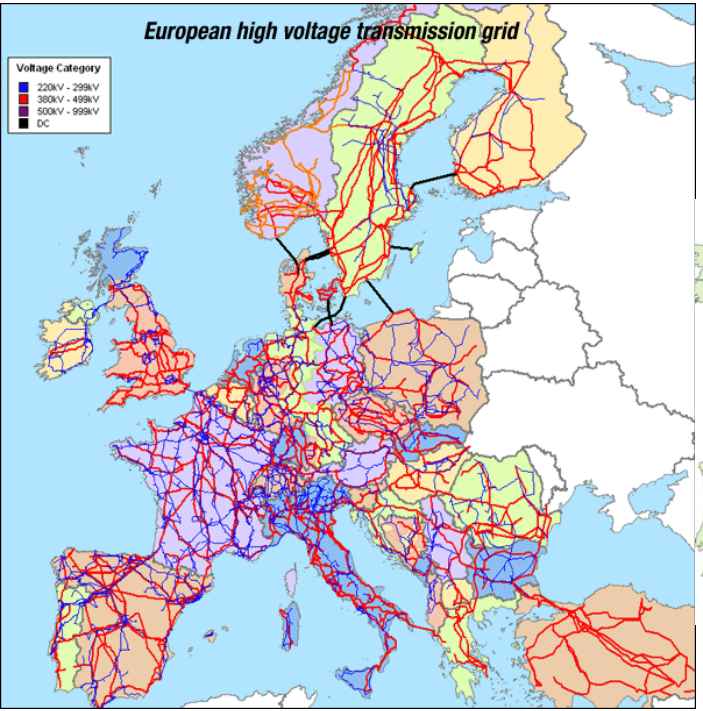
- Grundlegende Anforderungen werden festgelegt zwischen EVU und Hersteller
- Anlehnung an Europäische Standards und Normen (M441, M490, ENTSO)
- Schichtweise Erweiterung angedacht
- Aufkommender Fokus auf HW Security
- Behörden bauen Kapazitäten auf im Umfeld IT Security der volkswirtschaftlich relevanten Infrastrukturen
- Übertragungsnetze Anpassungen und Ausbau gemäss Europäischen Netzanforderungen

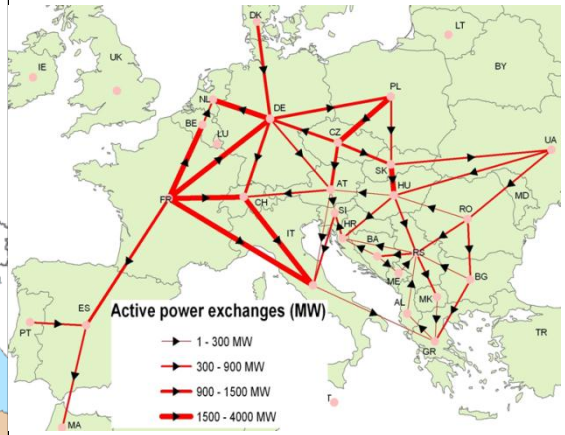
Situation Schweiz

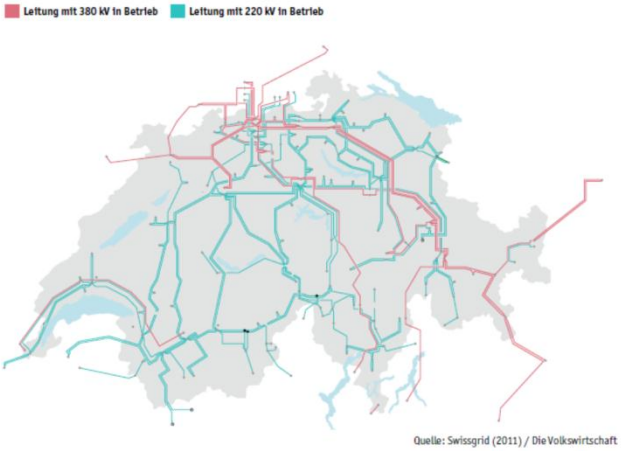
Die angestrebte Rolle…

- Stromdrehscheibe in Europa
- Gemeinschaftlicher Netzausbau
- Gemeinschaftliche Versorgungskonzepte
- Angebot an Speicher (Stauseen)
- Sicherheit im Netzmanagement

Die Schweizer Stromtrassen..







… eine internationale Angelegenheit

Smart Grid Security - Erfahrungen

- **Energienetzbetrieb findet im regulierten Umfeld statt→**
  - Kostenanerkennung vom Staatlichen Regulator (Elcom) basierend auf gesetzlichen Mindestanforderungen
  - Wo Mindestanforderungen bezüglich Sicherheit fehlen, haben Kosten gegenüber Sicherheit Priorität
- **Grosse Energie Versorger konnten und können es sich leisten spezifische Sicherheitskonzept zu entwickeln und Umzusetzen (Bsp. ErDF, Centrica, Iberdrola, Oncor, PG&E…)**
- **Sicherheit und Datenschutz für Smart Grid kann nur erreicht werden mit «security by design»; heisst vorgängig und nicht nachträglich implementieren**
- **Sicherheit und Datenschutz muss mit einer End-to-End Betrachtung spezifiziert werden**
- **EC Recommendation vom 9.3.2012 empfiehlt allen Mitgliedstaaten dass Datenschutz und Sicherheit auf legislativer Ebene eingefordert werden soll.**
- **Standards wie NISTIR, ISO 27009, Common Criteria etc. sollten angewendet werden**

Christian Meier
Product Manager
Landis+Gyr AG
Theilerstr. 1
6301 Zug

Tel. +41 41 935 6000
Mail: christian.meier@landisgyr.com