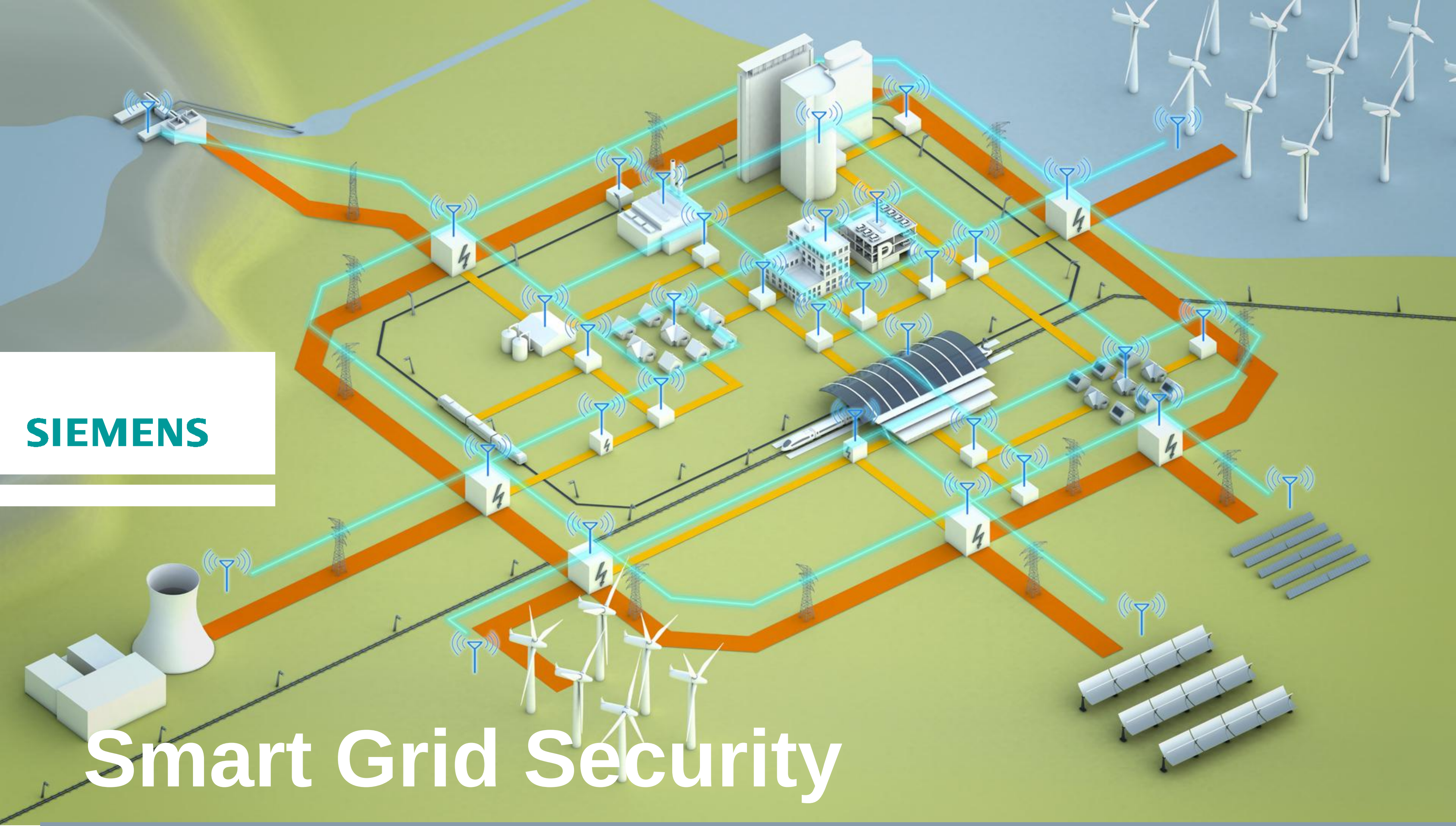


SIEMENS

Smart Grid Security

Protecting Intelligent Grid Control and Smart Metering

Summer School 2015 on Smart Energy Systems & Entrepreneurship
EIT ICT Labs & KIT. Karlsruhe, Germany. July 30th, 2015
Dr. David von Oheimb, Siemens AG, Corporate Technology

Most slides by Steffen Fries

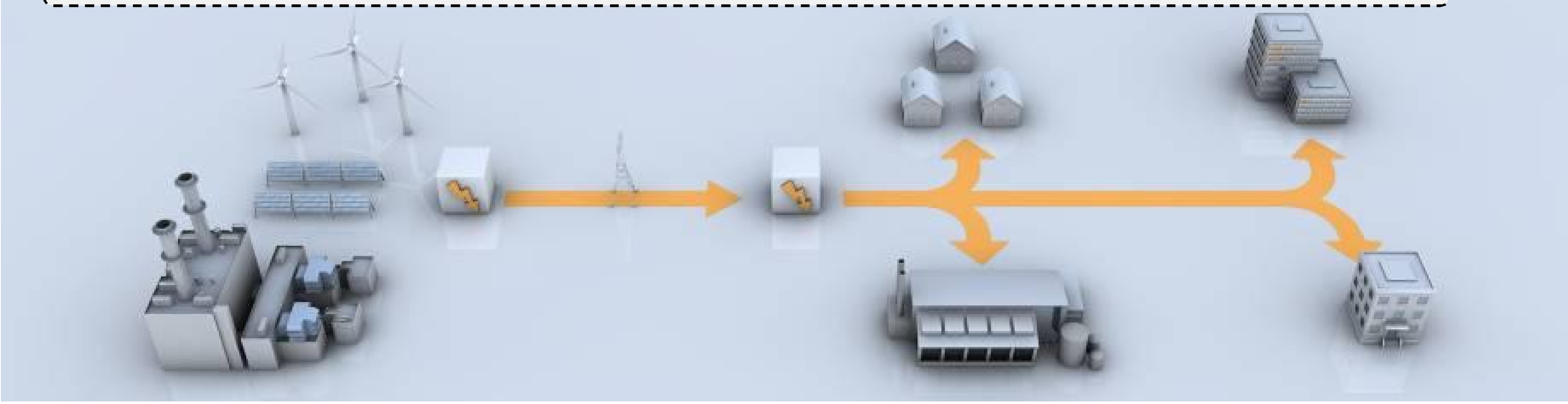
SIEMENS

Outline

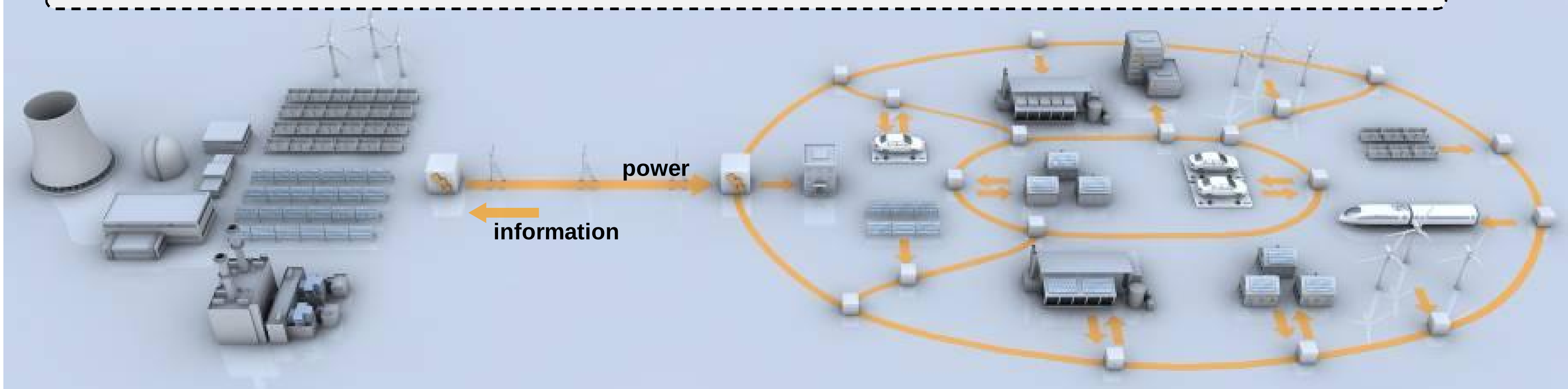
- **Smart Grid requires IT security**
- Specific security challenges
- Standardization & regulation
- Some technical details
- Research activities
- Summary

Conventional Grid is Evolving to Smart Grid Enabled by IT

Centralized generation, Unidirectional power flow

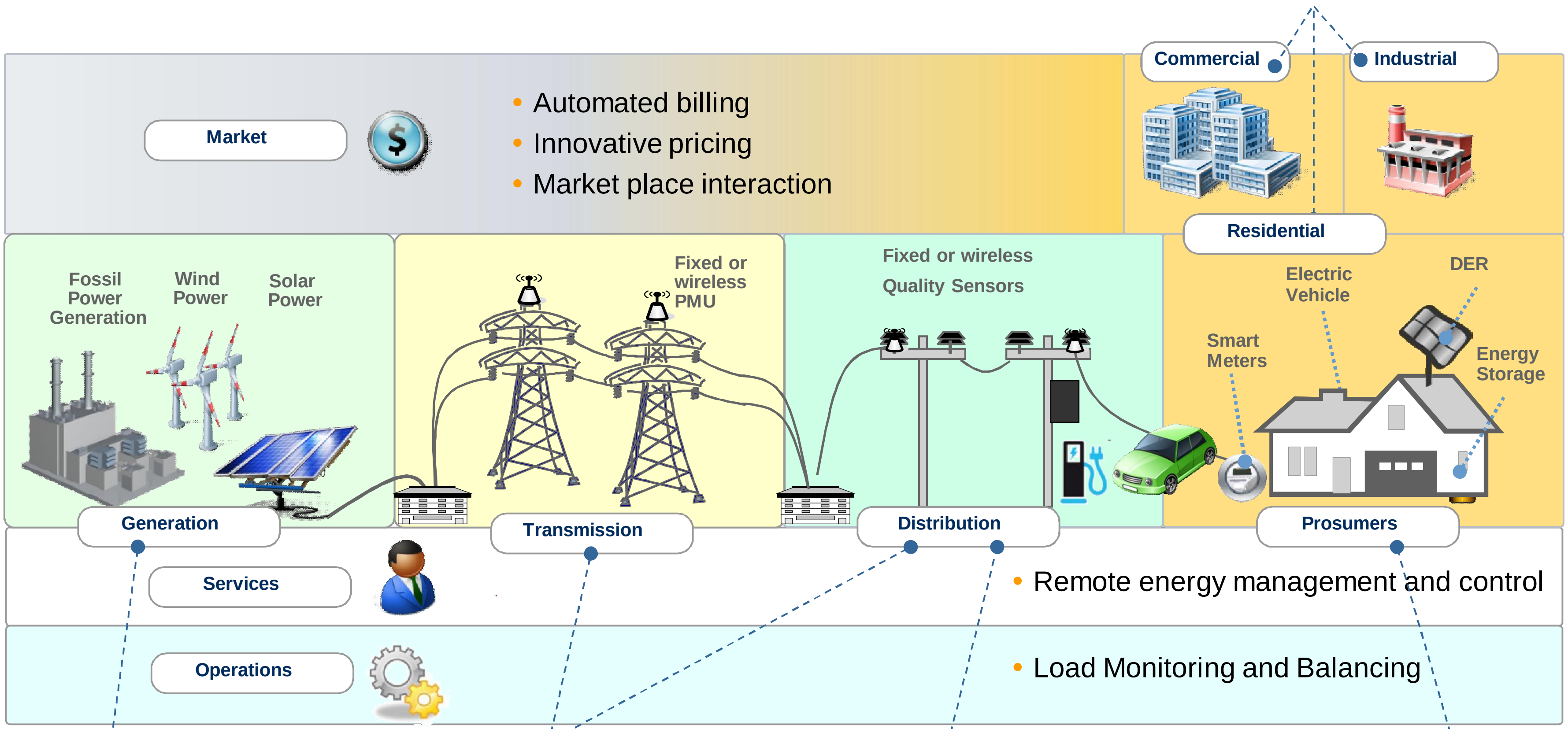


Centralized and decentralized generation, Bi-directional power flow → requires IT integration



Smart Grid Scenarios Where IT is Required

- Demand response management
- Micro grids



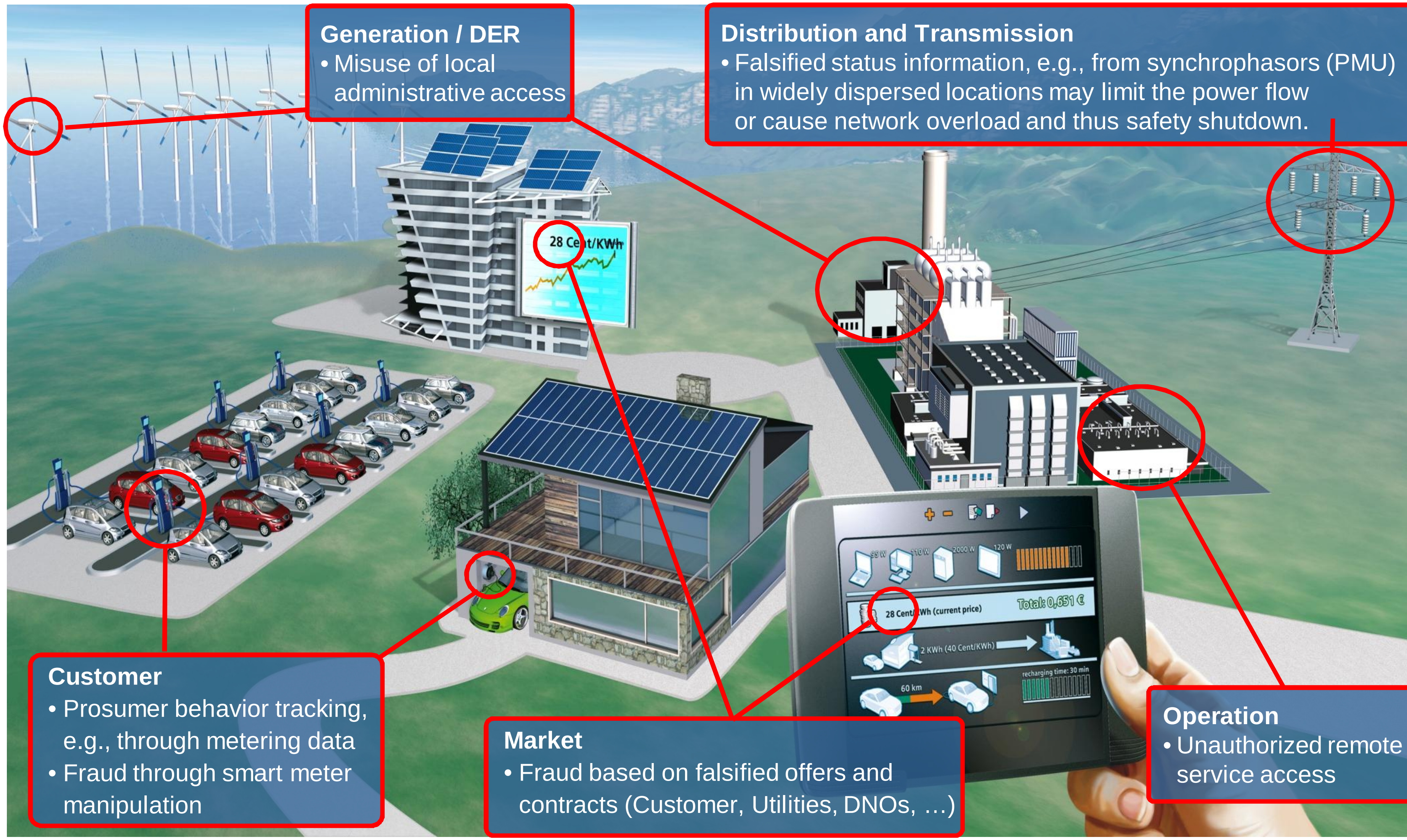
- Load balancing of power generation

- Real-time outage notification
- Power quality monitoring using **Phasor Measurement Units (PMUs)**

- Integration of **Distributed Energy Resources (DER)**
- Electro Mobility

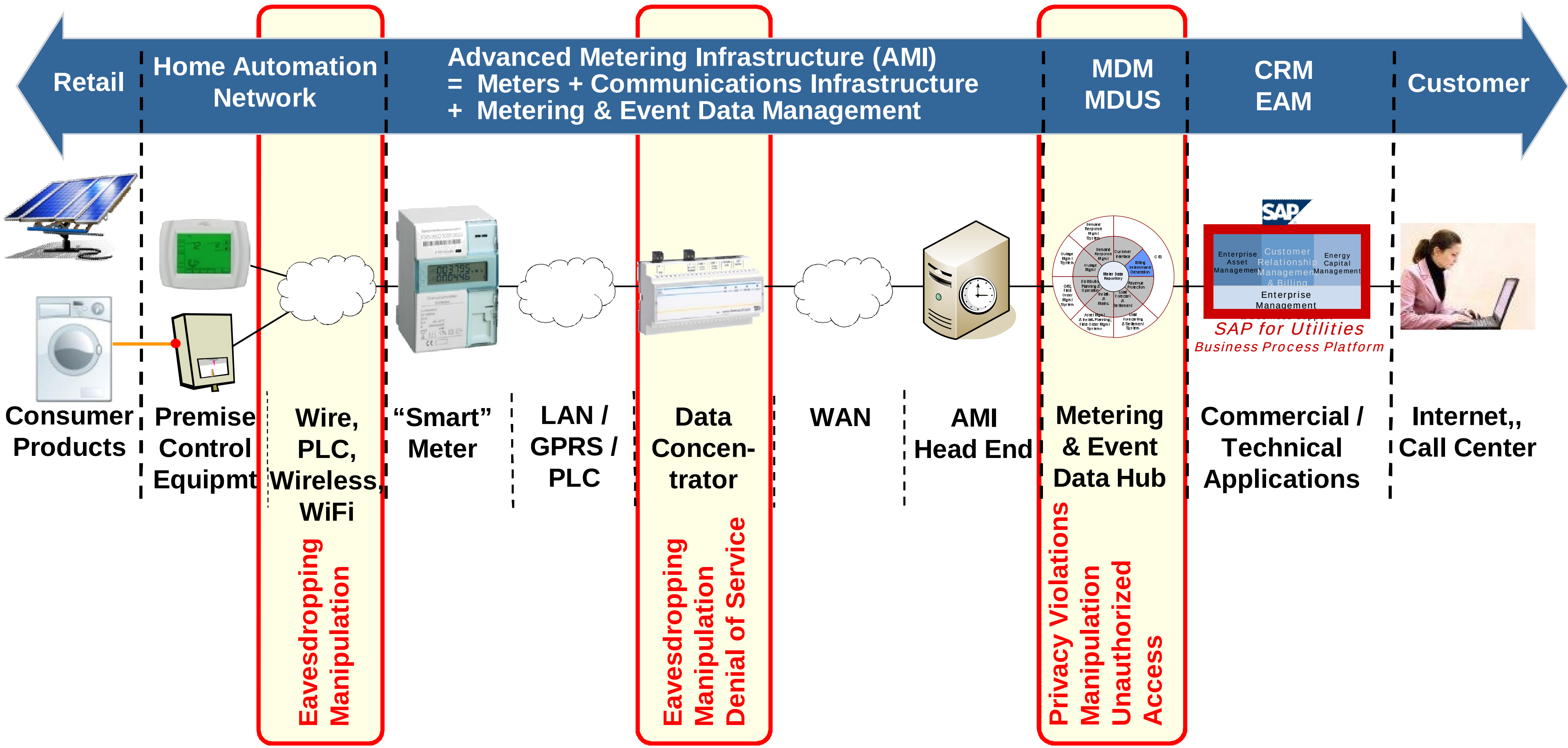
- Smart metering for consumption/generation
- Smart appliances

Security Requirements for Smart Grid Applications Stem From a Variety of Potential Attacks (examples)



Security threats on Smart Metering

Smart Metering: Distributed system defining data flows from prosumer to energy provider (with several subsystems, e.g., billing, notification, …) to third parties (e.g., marketing, manufacturer)



Outline

- Smart Grid requires IT security
- **Specific security challenges**
- Standardization & regulation
- Some technical details
- Research activities
- Summary

SIEMENS

Particular challenges of Smart Grid Security

Smart Grids are Cyber Physical Systems:

Strong mutual relation between physical and computational components
Physical security affects IT security and vice versa

70% of the existing energy grid is more than 30 years old *

Real-time and bandwidth requirements may limit protection mechanisms

Use of common off-the-shelf IT systems and networks
introduces all the usual cyber security vulnerabilities

80% to 90% of control centers are directly connected to the utility intranet

Large potential damage: power supply outage, maybe physical damage
to the grid, extra consumption, billing fraud, privacy leaks

Vulnerability, Exposure, Impact
High Risk

SIEMENS

Security Reality Check: incidents since 2000
Digital Attacks – Physical and Economic Harm

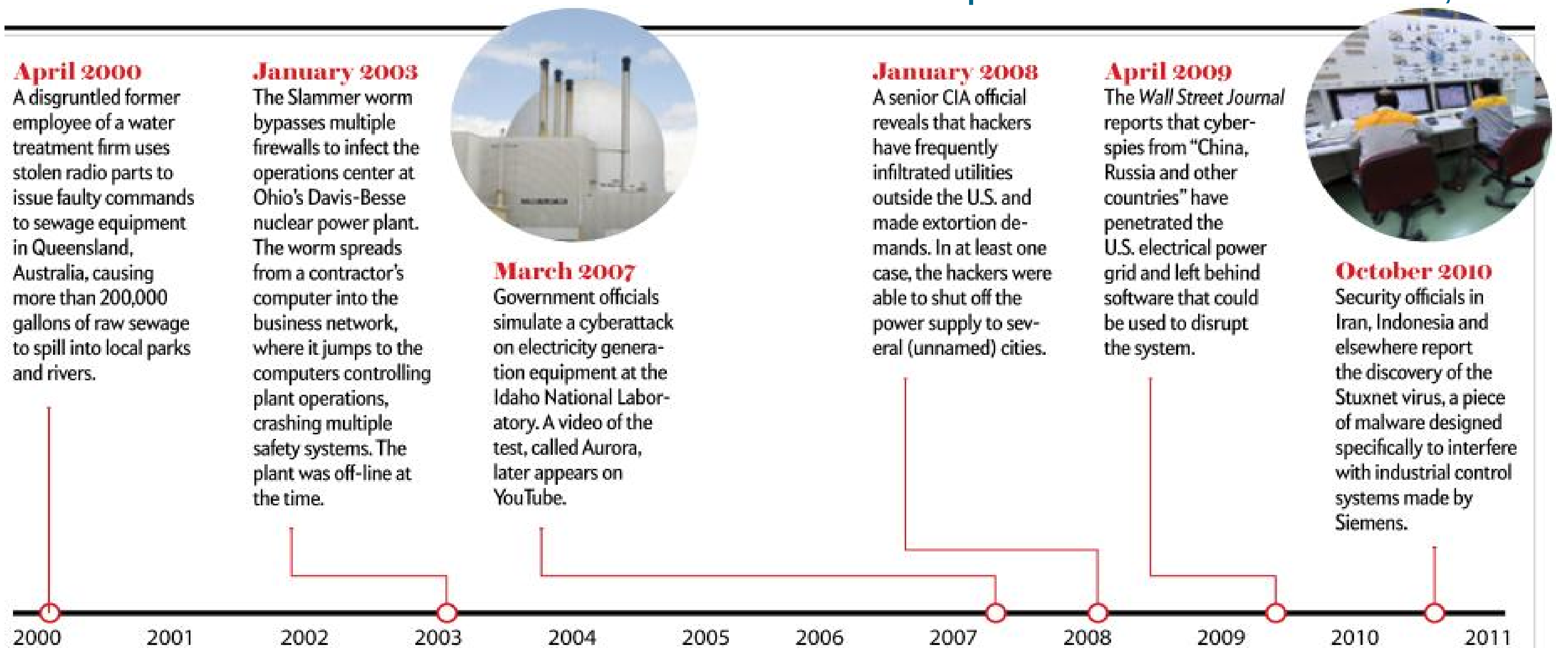
Misuse of Service

Virus Attack

Manipulation

Penetration

Viruses, Malware



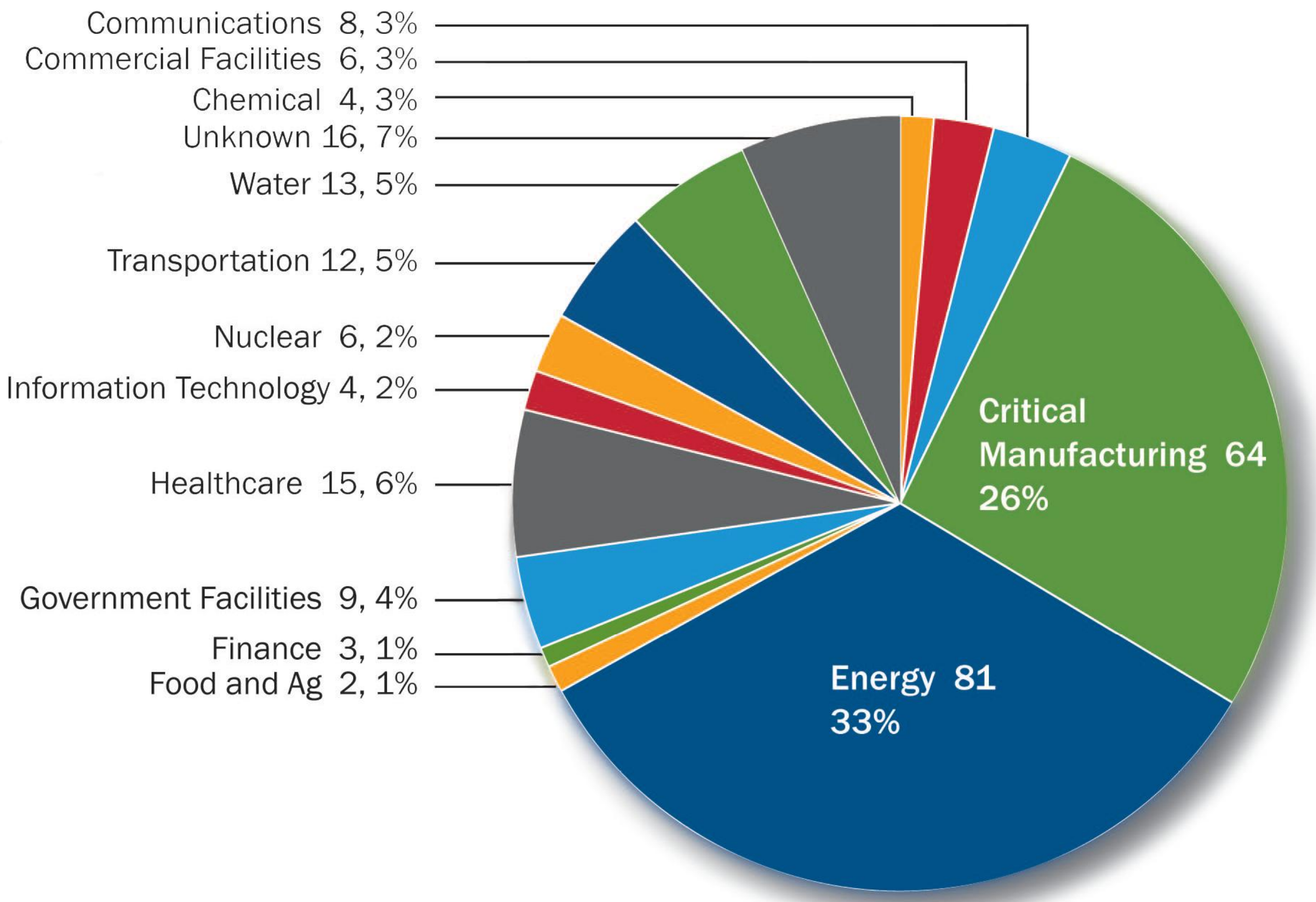
Source: Scientific American, July 20

Energy provider tests security – and fails
– Heise Security, April 8, 2014
http://www.heise.de/security/meldung/Energieversorger-testet-Sicherheit-und-faellt-durch-2165153.html

Dragonfly: Western Energy Companies Under Sabotage Threat
– Symantec, June 30, 2014
http://www.symantec.com/connect/blogs/dragonfly-western-companies-under-sabotage-threat?inid=us_ghp_hero2_dra

Popular electricity smart meters in Spain can be hacked, researchers say
– Reuters, October 7, 2014
http://uk.reuters.com/article/2014/10/07/cybersecurity-spain-idUKL6N0S20PM20141007

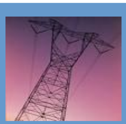
Energy Systems are Prime Targets in Critical Infrastructures



Source: ICS Report September 2014 – February 2015
The chart illustrates the number of ICS-CERT responses to sector specific cyber security threat across the critical infrastructure sectors. Any percentage total is the percentage as it relates to the total responses between 09/2014 - 02/2015.

Energy Automation Systems vs. Office World
Management & Operational Characteristics

SIEMENS

	Energy Control Systems 	Office IT 
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	Up to 30 years	3-5 years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular / scheduled
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x …	Medium, delays accepted
Non-Repudiation	High	Medium

Typical Data Exchanged in Smart Grid Applications and Their Security Impact

SIEMENS

Information asset	Description, potential content	Security impact
Control Commands	Actions requested by one component of other components via control commands. These commands may also include Inquiries, Alarms, Events, and Notifications.	Effects on system stability and reliability and also safety
Configuration Data	Configuration data (system operational settings and security credentials but also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behavior of a component and may need to be updated remotely.	Effects on system stability and reliability and also safety
Time, Clock Setting	Time is used in records sent to other entities. Phasor measurement directly relates to system control actions. Moreover, time is also needed to use tariff information optimally. It may also be used in certain security protocols.	Effects on system control (stability and reliability and also safety) and billing
Access Control Policies	Components need to determine whether a communication partner is entitled to send and receive commands and data. Such policies may consist of lists of permitted communication partners, their credentials, and their roles.	Effects on system control and influences system stability, reliability, and also safety
Firmware, Software, and Drivers	Software packages installed in components may be updated remotely. Updates may be provided by the utility (e.g., for charge spot firmware), the car manufacturer, or another OEM. Their correctness is critical for the functioning of these components.	Effects on system stability and reliability and also safety
Customer ID and location data	Customer name, identification number, schedule information, location data	Effects on customer privacy
Meter Data	Meter readings that allow calculation of the quantity of electricity consumed or supplied over a time period and may be used for controlling energy loads but also for interactions with an electricity market.	Effects on system stability and billing
Tariff Data	Utilities or other energy providers may inform consumers of new or temporary tariffs as a basis for purchase decisions.	Effects on customer privacy and also competition

Outline

- Smart Grid requires IT security
- Specific security challenges
- **Standardization & regulation**
- Some technical details
- Research activities
- Summary

Security Solutions (Architectures) Target Multiple Layers of Defense

Comprehensive security architecture, including technical, physical and organizational means

Organizational Security

Personnel services to protect assets

- Develop, maintain and enforce Security Policy
- Manage user accounts
- Security system provisioning and maintenance
- Security patrols

Physical Security

Physical access to equipment and network

- Restricted access to equipment rooms, closets, etc.
- Locations of wall jack, wireless hot-spots, etc.
- Video surveillance
- Intrusion detection systems and alarms

Professional Services: Analyses, Consulting…

Device Security

Protection of system components

- OS Hardening
- User authentication and authorization
- Securing communication interfaces (cryptography)
- Event logging

Network Security

Protection of network infrastructure

- Traffic separation using VLANs, VPNs, etc.
- ACLs control connectivity between components
- Use of Firewalls, SBCs, IDS, IPS, etc.

Lifecycle services

OEM Security Products

Dedicated security products for networks & systems

Managed Security Services

Security Policy Framework

Security Guidelines / Standards / Regulation Ensure Reliable Operation of Smart Grids (examples)

SIEMENS

NIST National Institute of Standards and Technology U.S. Department of Commerce

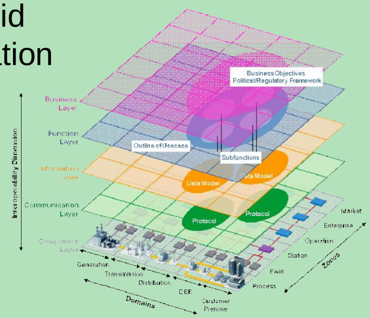
SGIP

Smart Grid Interoperability Panel, Cyber Security WG
→ NIST IR 7628

Cyber Security Framework

cen CENELEC ETSI

Smart Grid Coordination Group → SGAM



FERC FEDERAL ENERGY REGULATORY COMMISSION

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Infrastructure Protection
CIP 001-011

Bundesamt für Sicherheit in der Informationstechnik

- Protection Profile for SM GW
- Guideline TR-03109 required by EnWG (Energy Industry Act)

- Critical Infrastructure Protection

IEC ISO

ISO JTC 1 IEC INFORMATION TECHNOLOGY STANDARDS

- IEC TC 57 – Power systems management and associated information exchange
  → IEC 62351-1 … -13
- IEC TC 65 – Industrial Process Measurement, Control and Automation
  → IEC 62443-1 … -4
- ISO/TC 022/SC 03 & IEC/TC 69 JWG 01 – Vehicle-to-Grid Interface
  → Security integral part of ISO 15118

- ISO 27001 – Information technology - Security techniques - Requirements
- ISO 27002 – Code of Practice for information security management
- ISO 27019 – Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002

Note: the stated organizations and standards are just examples and are not complete

Regulation Example

Smart Grid Control: NERC CIP – Critical Infrastructure Protection Standards

- **North American Electric Reliability Corporation (NERC)**: Non-Profit Organization in the U.S.
- **Specifies the minimum security requirements** to ensure the security of the **electronic exchange of information** for supporting the bulk power system
- **Unified format** (intro, rules, measures, compliance or deviation, regional specifics and history)

Scope

Physical Security	Cyber Security	Security Operations
Video, Access Control, Media Management	Authorization, Integrity, Segmentation	Authorization, Integrity, Segmentation

Parts

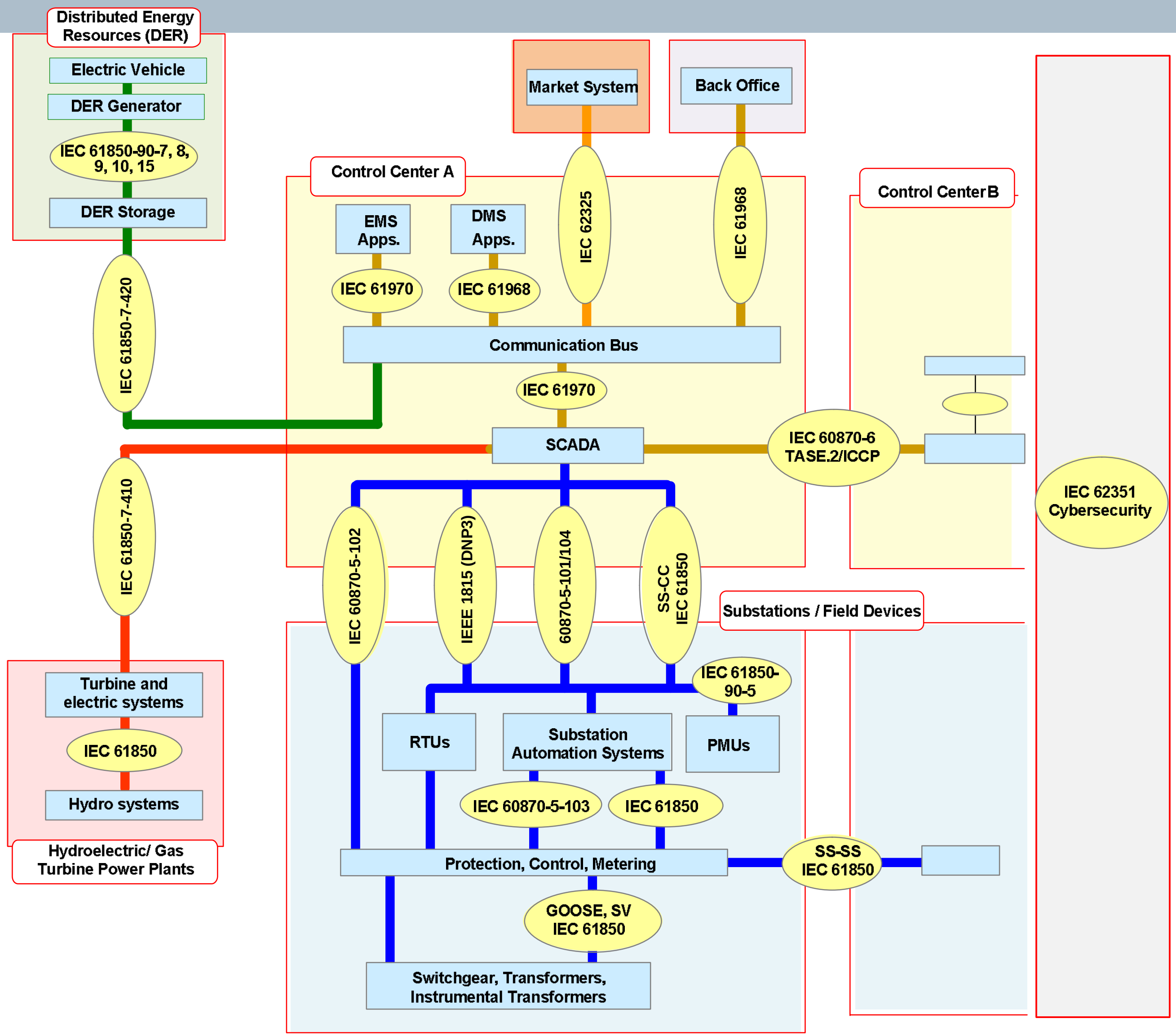
- Sabotage Reporting
- BES Cyber System Categorization
- Security Management Controls
- Personnel and Training
- Electronic Security
- Physical Security
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for BES Cyber Systems
- Configuration Change Management and Vulnerability Assets.
- Information Protection

- Binding for operators of power systems in USA, Canada and Mexico targeting auditable compliance
  → Compliance process based on **self audit**, which must be repeated yearly
- **Verification** through a local NERC auditor, correction within 30 days required.

SIEMENS

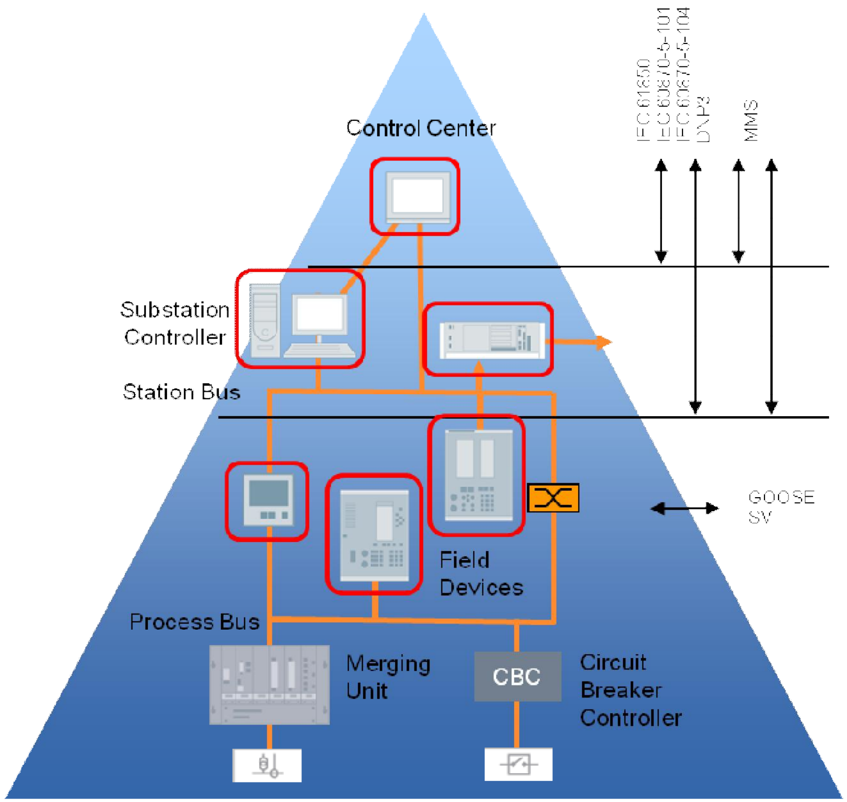
Core Communication Standards for Smart Grids – IEC TC57 Reference Architecture

- **IEC 61970 / 61968**
  Common Information Model (CIM)
- **IEC 62325**
  Market Communication using CIM
- **IEC 61850**
  Substation & DER Automation
- **IEC 60870**
  Telecontrol Protocols
- **IEC 62351**
  Security for Smart Grid



SIEMENS

IEC 62351 Specified by IEC TC57 WG15 – Enables Secure Modern Energy Control Networks



IEC 62351-		IEC 62351-	
1	Introduction and overview	7	Network and system management
2	Glossary of terms	8	RBAC for Power systems management
3	Profiles Including TCP/IP	9	Key Management
4	Profiles Including MMS	10	Security Architecture Guidelines
5	Security for IEC 60870-5 and Derivatives	11	Security for XML Files
6	Security for IEC 61850 Profiles		

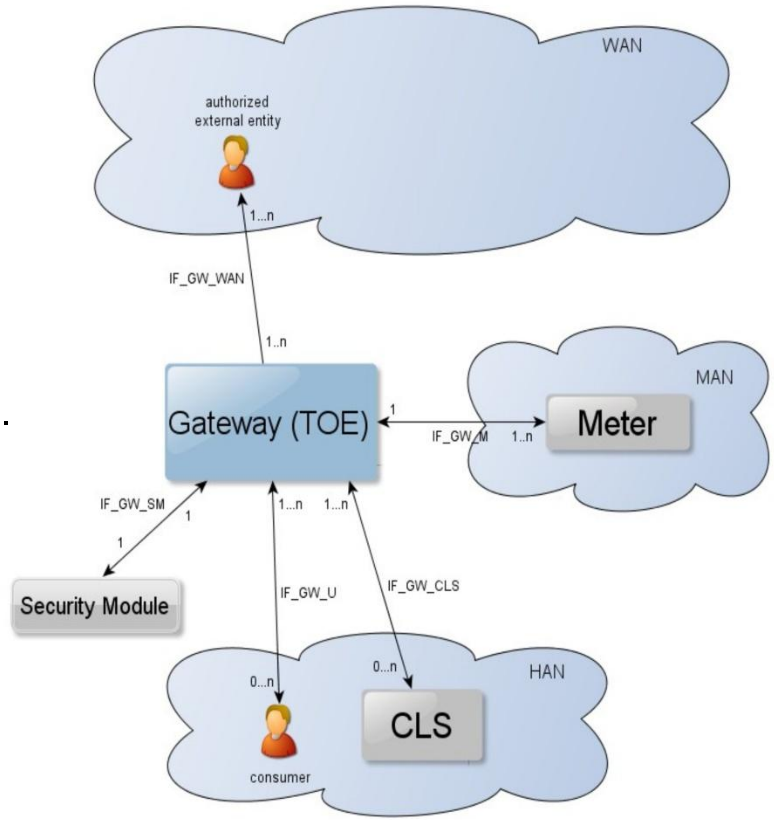
- **Approach**
  - *Umbrella standard* consisting of several parts targeting dedicated security measures
  - Targets IEC 61850, IEC 60870-5-101, IEC 60870-5-104, and also IEEE 1815 (DNP3)
- **Scope**
  - **Integrity/Encryption** of data exchanged over networks using ***Transport Layer Security (TLS)*** on TCP/IP based links and integrity protection using HMAC on serial links
  - **Authenticating applications** using strong authentication via the exchange of ***public keys*** and ***digital certificates,*** but also on ***symmetric keys***
  - **Focus on end-to-end security**

Regulation Example

Smart Metering: German BSI Smart Meter Gateway Protection Profile

SIEMENS

- German Federal Office for Information Security (BSI) was commissioned by the BMWi in 2010 to develop a security requirements specification for smart meter gateways.
- Target of the specification/security evaluation (ToE):
  - Communication gateway between devices of private and commercial consumers and service providers (mostly for electricity, but also other gas, water).
  - Responsible for collection and local processing of meter data and secure distribution of this data to external parties.
- Protection Profile based on Common Criteria for information security technology evaluation (ISO 15408)
- Accompanying technical guideline TR 03109
- Builds on a hardware security module as trust anchor
- German Energy Industry Act (EnWG) requires application of smart meter complying to the BSI SM PP and TR 03109 in environments with an annual energy consumption of more than 6000 kWh starting 2013.
- Release published March 2013
  → EnWG application dates adopted



Protection Profile for the Gateway of a Smart Metering System (Gateway PP), BSI, Version 1.0.1, 11/2011

SIEMENS

Comments on the BSI’s SM GW Protection Profile

- Clear security requirements for the gateway
- High assurance level of critical system component
- Strong national standard ensuring interoperability
- Overall system security not in scope
- Communication real-time requirements and DoS protection not addressed
- Technical restrictions: point-to-point connections only (no multicast)
- Hardware Security Module integration ill-designed (authentication of use)
- Use of classical PKI introduces critical central points of failure
- Technical overhead: Multiple layers of protection, full-blown PKI, mandatory use of HW security module
- High costs per gateway and overall system, for installation and operation

Outline

- Smart Grid requires IT security
- Specific security challenges
- Standardization & regulation
- **Some technical details**
- Research activities
- Summary

Communication Security Provided the Naïve Way: RFC 3514 “The Security Flag in the IPv4 Header”

Sounds good, but sadly, it’s a joke!

Informational RFC (01.04.2003), Steve Bellovin (AT&T labs)

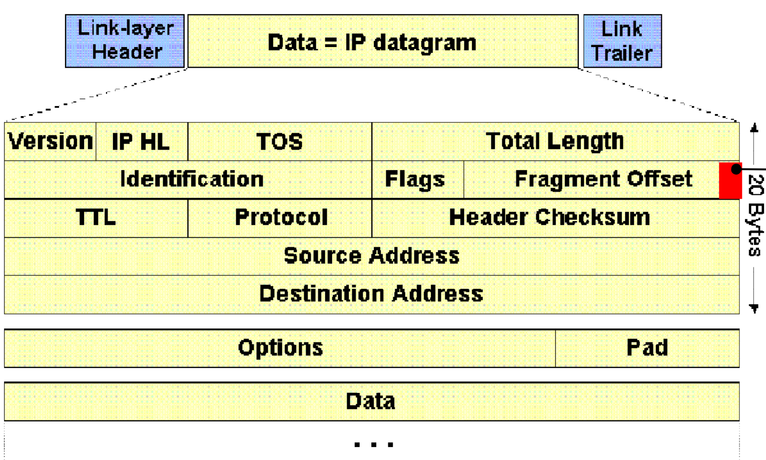
Basic Idea

- Detection of packets with malicious content on intermediate systems

  → addresses Firewalls, IDS systems, and packet filters

Concept

- Usage of the unused high-order bit of the IPv4 fragment offset field to signal malicious content
- For IPv6 options header conveys 128 bit strength indicator



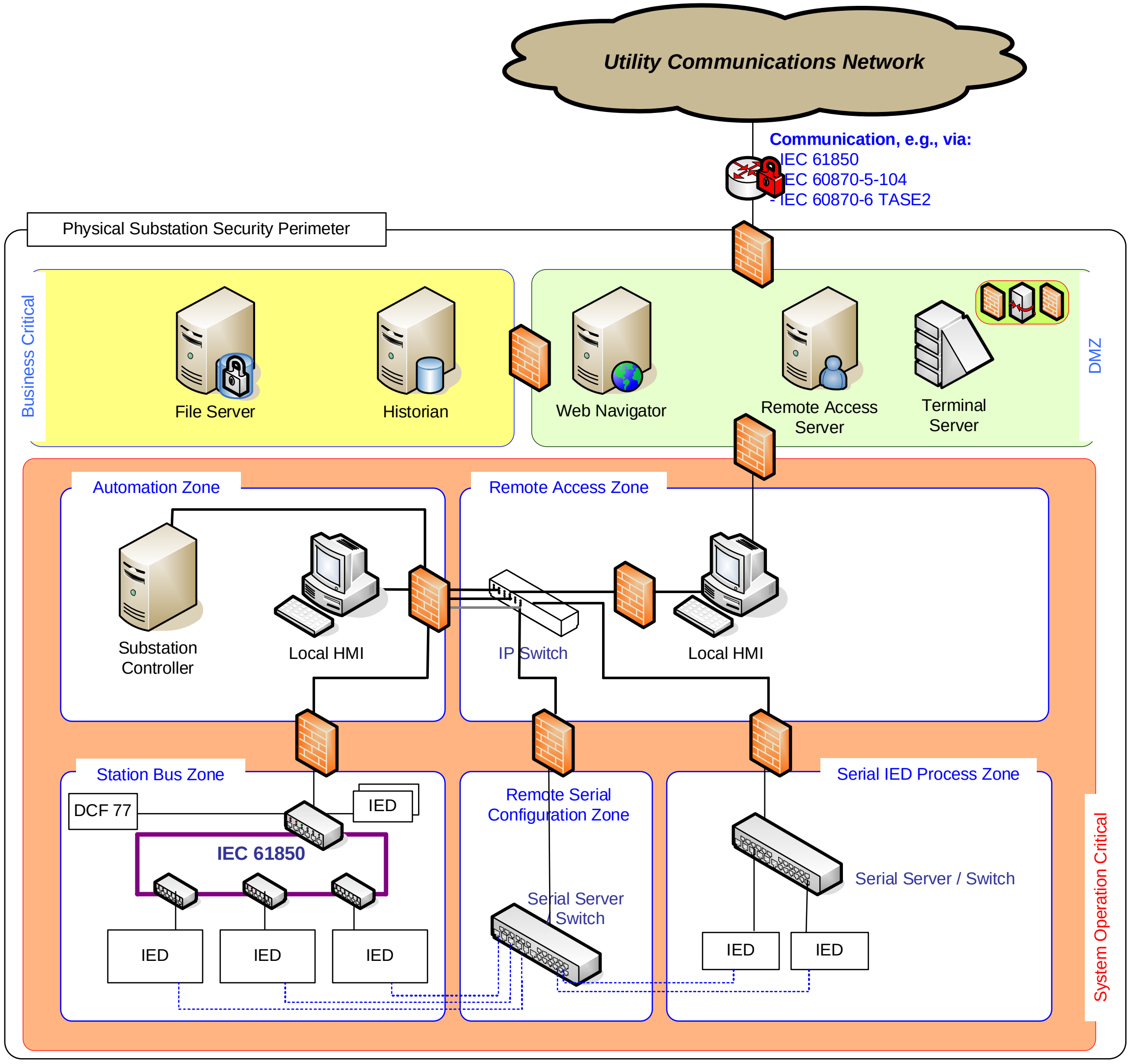
Evil Flag

- 0x00 – packet has no evil content
- 0x01 – packet has evil content

Continuous Improvements at the Example of IEC 62351–6 (GOOSE and SV Security)

SIEMENS

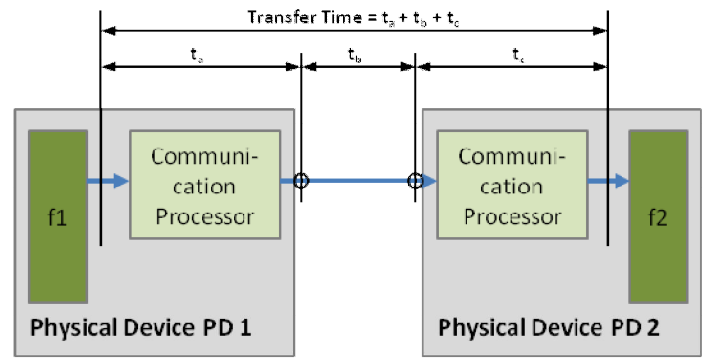
- Targets communication of **Generic Object Oriented Substation Events (GOOSE),** and **Sample Values (SV)** using, e.g., plain Ethernet.
- Usage of **multicast transfer** (device local subscription for events)
- Security required in terms of message integrity and source authentication
- Standard currently employs **digital signatures**
- **BUT …**



Selected Security Approach Does Not Fit the Specific Needs

SIEMENS

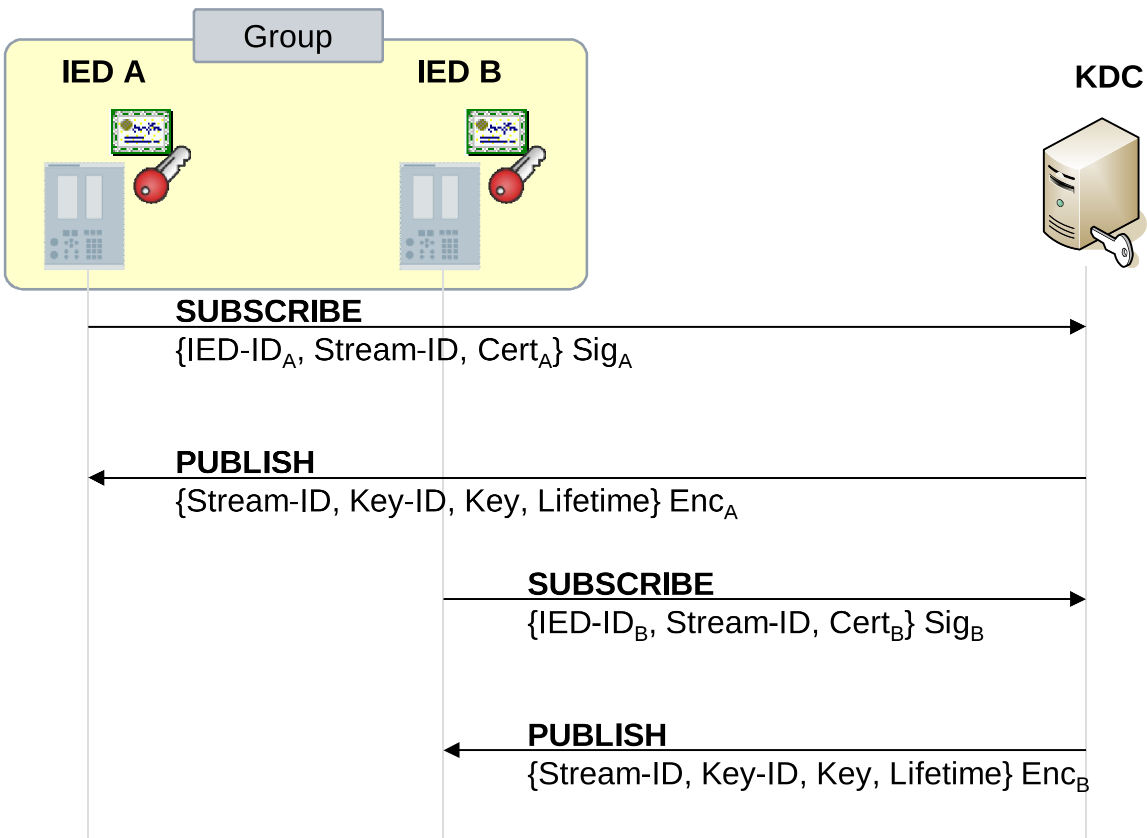
- GOOSE – control model mechanism in which any format of data (status, value) is grouped into a data set and transmitted as set of substation events.
- **Strong real-time requirements**:
  sample rate of 80 samples per power cycle, thus
  4000 packets per second for usual 50 Hz frequency
- Selected security approach: using digital signatures:
  - Good from a cryptographic point of view
  - Typical field devices do no meet the performance requirements
- Alternative approach using group based security:
  - Depends on a keyed hash involving a group key
  - Lacks ability to identify single rogue device



Type	Definition	Timing Requirements
1	**Fast messages** contain a simple binary code containing data, command or simple message, examples are: “Trip”, “Close”, etc.	See Type 1a and 1 b below
1A	**TRIP** – most important message	– P1: transfer time shall be in the order of half a cycle. → 10 ms – P2/3: transfer time shall be below the order of a quarter of a cycle. → 3 ms
1B	**OTHER** – Important for the interaction of the automation system with the process but have less demanding requirements than trip.	– P1: transfer time < 100ms – P2/3: transfer time shall be below the order of one cycle. → 20 ms

Group based Key Management provides solution for Substation and Wide Area GOOSE/SV

- Application of a group based key to achieve message integrity for Intelligent Electronic Devices (IED).
- IEDs authenticate towards KDC using IED- specific certificates and corresponding private keys
- Key Management based on Group Domain of Interpretation (GDOI, RFC 6407)



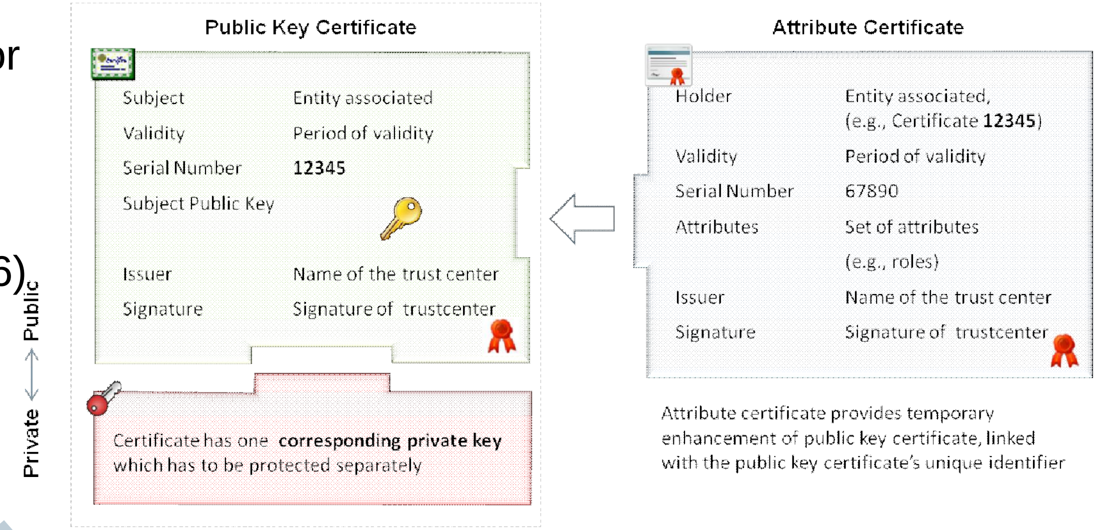
Key Distribution Center (KDC)
- pre-configured data stream related IED access list
- different data streams
- generates data stream related (group) keys
- May by realized as component within a distinct IED

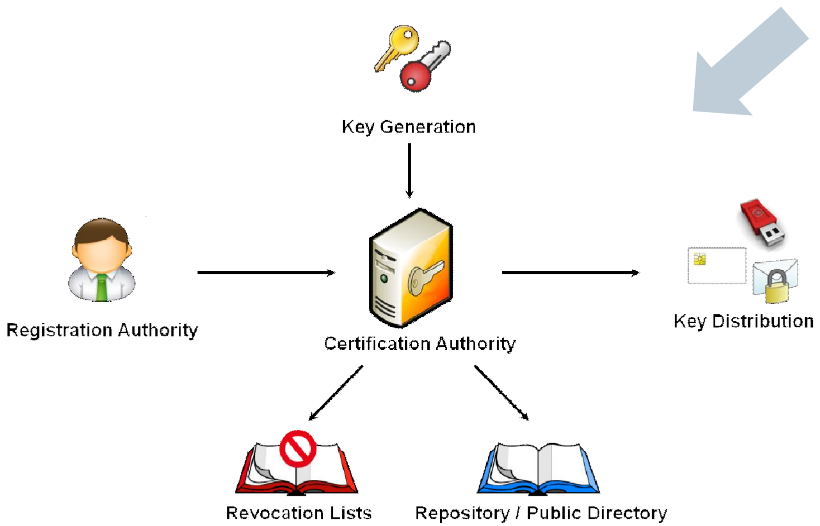
IEC 62351–9 Key Management Specifically Addresses the Handling of Asymmetric Key Material

SIEMENS

X.509 key material used in IEC 62351 for

- **Message protection** on transport or application layer (3, 4, 5, 6, 11)
- **distribution of symmetric keys** (5, 6)
- **realize RBAC** in conjunction with attribute certificates (8)





- **Public Key Infrastructure (PKI)** provides means to manage X.509 key material for users and IEDs
- IEDs ideally generate key material, only certification is done by the CA
- Human users apply for a certificate; Key generation either through tokens or PKI
- **Migration option** via self-signed certificates in conjunction with certificate whitelisting

IEC 62351–8 (TS)
Predefined Roles

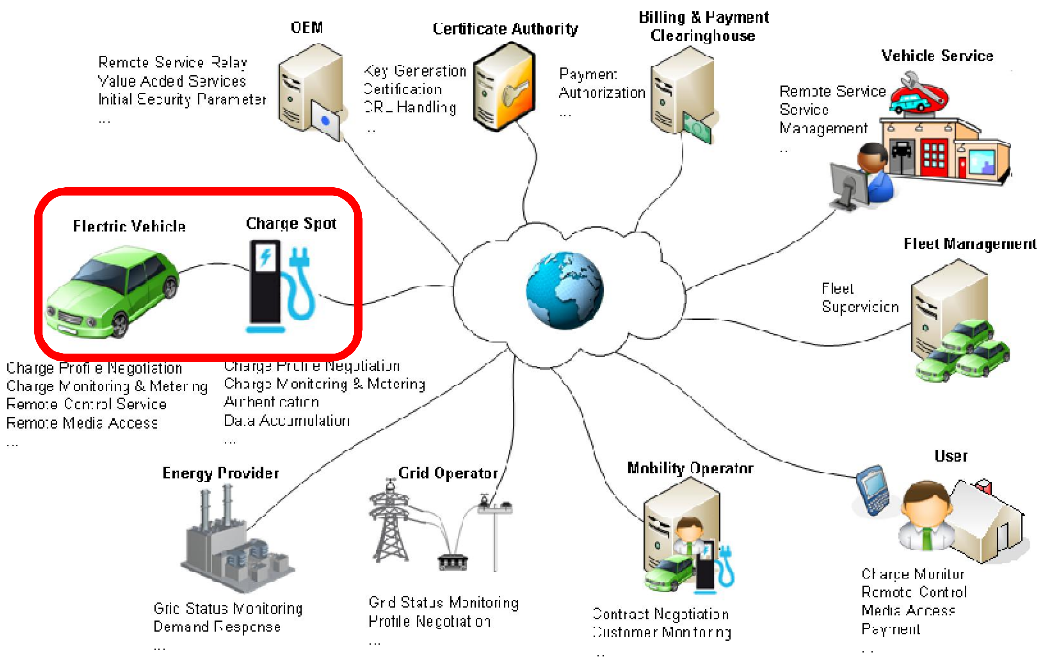
- **VIEWER:** can view what objects are present within a Logical-Device by presenting the type ID of those objects.
- **OPERATOR:** can view what objects and values are present within a Logical-Device by presenting the type ID of those objects as well as perform control actions.
- **ENGINEER:** can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an engineer has full access to DateSets and Files and can configure the server locally or remotely.

Value	Right / Role	VIEW	READ	DATASET	REPORTING	FILEREAD	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTINGGROUP	SECURITY
<0>	VIEWER	X			X							
<1>	OPERATOR	X	X		X				X			
<2>	ENGINEER	X	X	X	X		X	X		X		
<3>	INSTALLER	X	X		X		X			X		
<4>	SECADM	X	X	X			X	X	X	X	X	X
<5>	SECAUD	X	X		X	X						
<6>	RBACMNT	X	X					X		X	X	
<7…32767>	Reserved	For future use of IEC defined roles.										
<-32768…-1>	Private	Defined by external agreement. Not guaranteed to be interoperable.										

- **INSTALLER:** can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.
- **SECADM:** can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and validity periods; change security setting such as certificates for subject authentication and access token verification.
- **SECAUD:** Security auditor can view audit logs.
- **RBACMNT**: can change role-to-right assignment.

SIEMENS

Security in ISO/IEC Standardization of Vehicle to Grid Communication Interface as part of IEC 15118



Security is the essential building block to ensure **safe charging** and **correct billing** of electrical vehicles connected to the smart power grid

Approach

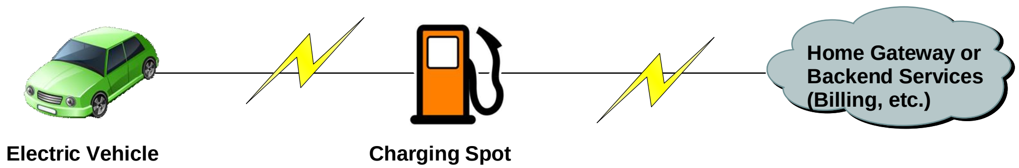
- Joint ISO/IEC (IEC TC69 JWG01) activity to **standardize** the interface between vehicle and charging station
- Start: Security Analysis of use cases to determine security requirements
- Definition of a security solution with **reuse** of existing security technologies

Scope

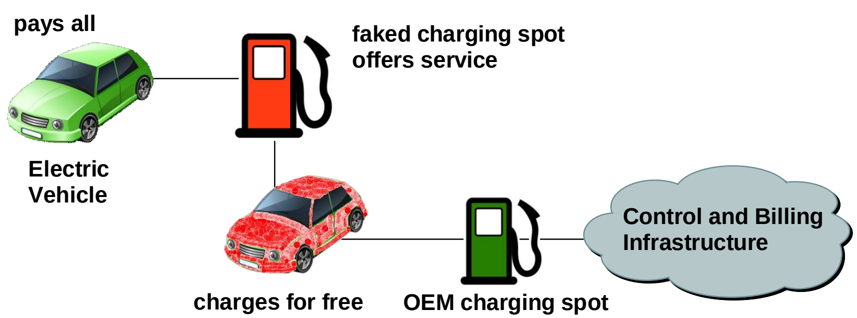
- Communication security services like authentication, communication integrity and confidentiality
- for vehicle to charging spots but also deeper into the backend (e.g., to billing, services, mobility operator)
- Ease of use

Example Threats to a Charging Infrastructure Targeting the Vehicle-to-Grid Interface

1. **Eavesdropping or Interception**

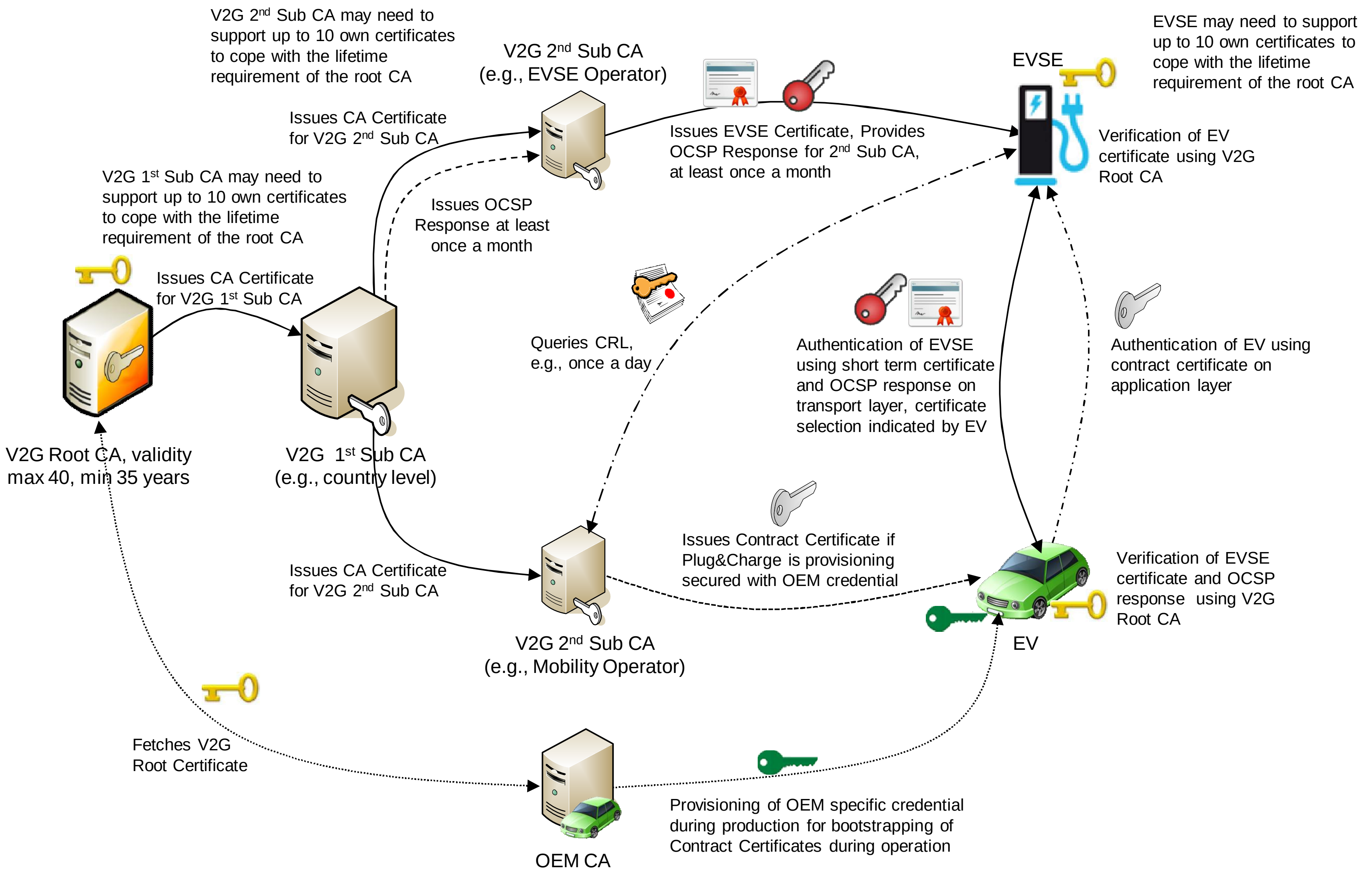


2. **Man-in-the-Middle Attack**



3. **Transaction Manipulation or Falsifying**
4. **Transaction Repudiation**
5. **Attack network from within vehicle**

IEC 15118 – Credential Handling During Operation (Example Based on Current State)



Outline

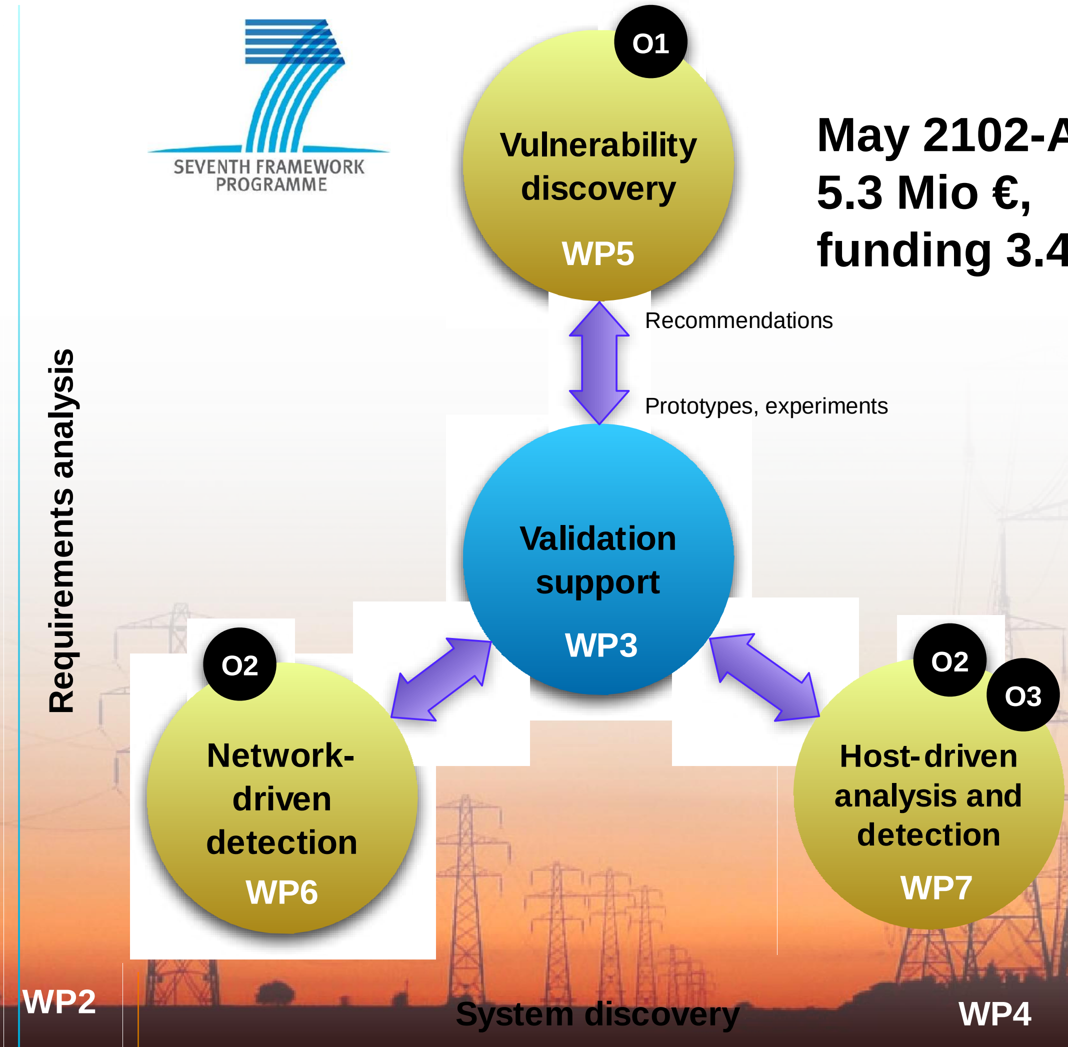
- Smart Grid requires IT security
- Specific security challenges
- Standardization & regulation
- Some technical details
- **Research activities**
- Summary

EU FP7 Project CRSIALIS: Securing Critical Infrastructures

CRISALIS
SECURING CRITICAL INFRASTRUCTURES

SIEMENS

SEVENTH FRAMEWORK PROGRAMME



May 2102-Aug 2015,
5.3 Mio €,
funding 3.4 Mio €

CRISALIS objectives:

- **O1** Securing the systems
- **O2** Detecting intrusions
- **O3** Analyzing successful intrusions

CRISALIS consortium:

Security industry

Symantec. SECURITY MATTERS

Control system industry/end users

Enel alliander SIEMENS

Academia

EURECOM Sophia Antipolis
UNIVERSITY OF TWENTE.

Outline

- Smart Grid requires IT security
- Specific security challenges
- Standardization & regulation
- Some technical details
- Research activities
- **Summary**

Summary

Current state

- **Machine-2-machine connectivity down to field devices** is a major driver for the Smart Grid
- **Security has been acknowledged as crucial** to realize Smart Grid
- **Standards provide technical security solutions** for dedicated parts of the Smart Grid
- **Regulation and guideline documents are available** and are being further evolved
- **Research is addressing Smart Grid security** in several funded projects

Challenges for IT security

- Coordination and alignment of requirements from **plurality of stakeholders** (utilities, consumers, IT, etc.)
- Coping with **differences in innovation speed**, in particular Smart Metering: vs. Energy Management
- **Political influence** → Regulated markets; e.g., EU mandates M441 M490
- Migration from **legacy environments** not well supporting appropriate IT security
- Security has to cope with **domain specific characteristics** (device capabilities, multicast, …)
- **Device-oriented security and identity infrastructure** (processes, scalability, limits of authority, …) supporting efficient creation, distribution and handling of cryptographic credentials (e.g., security modules and their integration into products & production)

Thank you for the attention!
- Questions?