Corporate Technology

SIEMENS

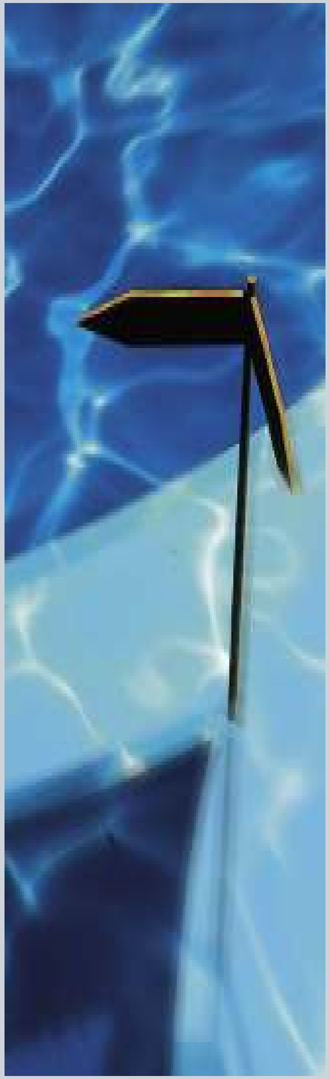
Securing the Smart Grid

Steffen Fries

Siemens AG, CT T, GTF IT Security
☎ : +49 89 636 53403
💻 : steffen.fries@siemens.com

© Siemens AG, Corporate Technology, May 2011

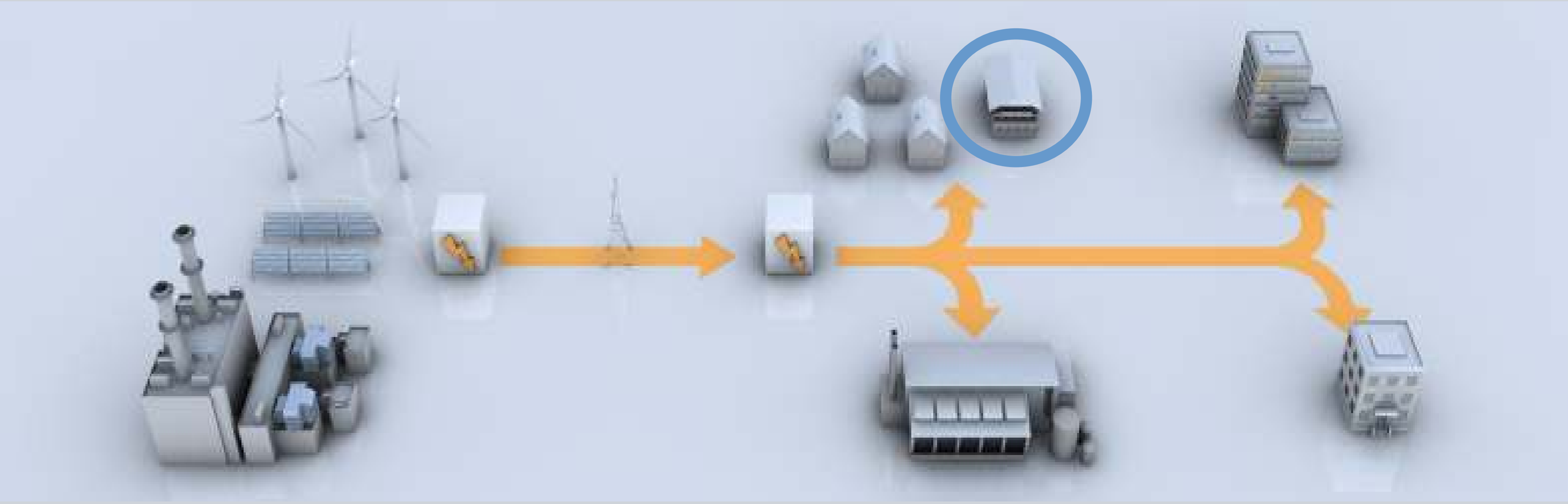
Outline



- Smart Grid – What is it all about?
- Smart Grid Scenarios and Components
- The need for Cyber Security
- Standardization & Regulation
- Research Activities
- Summary & Challenges

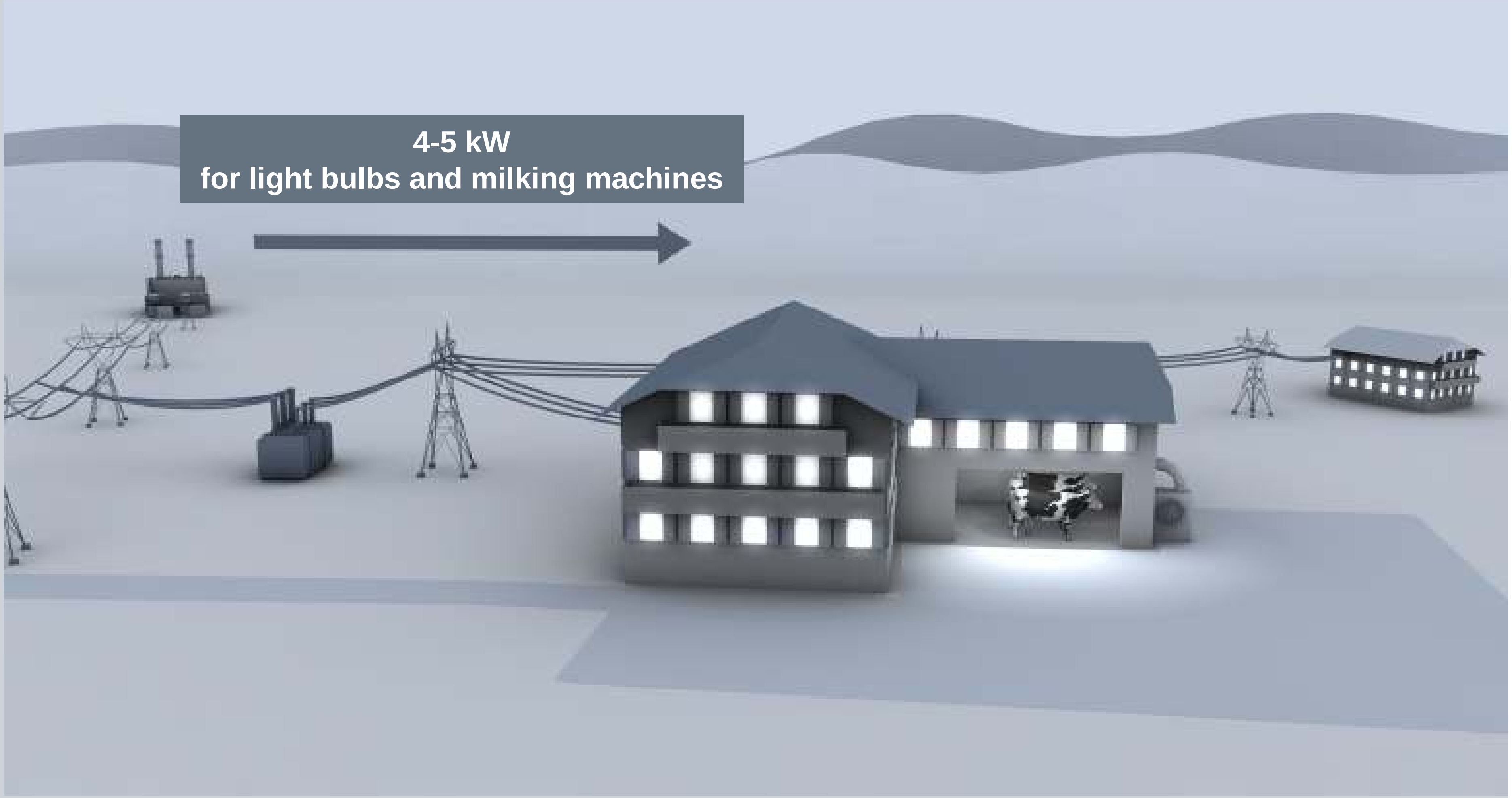
© Siemens AG, Corporate Technology

Power systems are in transformation – The energy system as we know it…



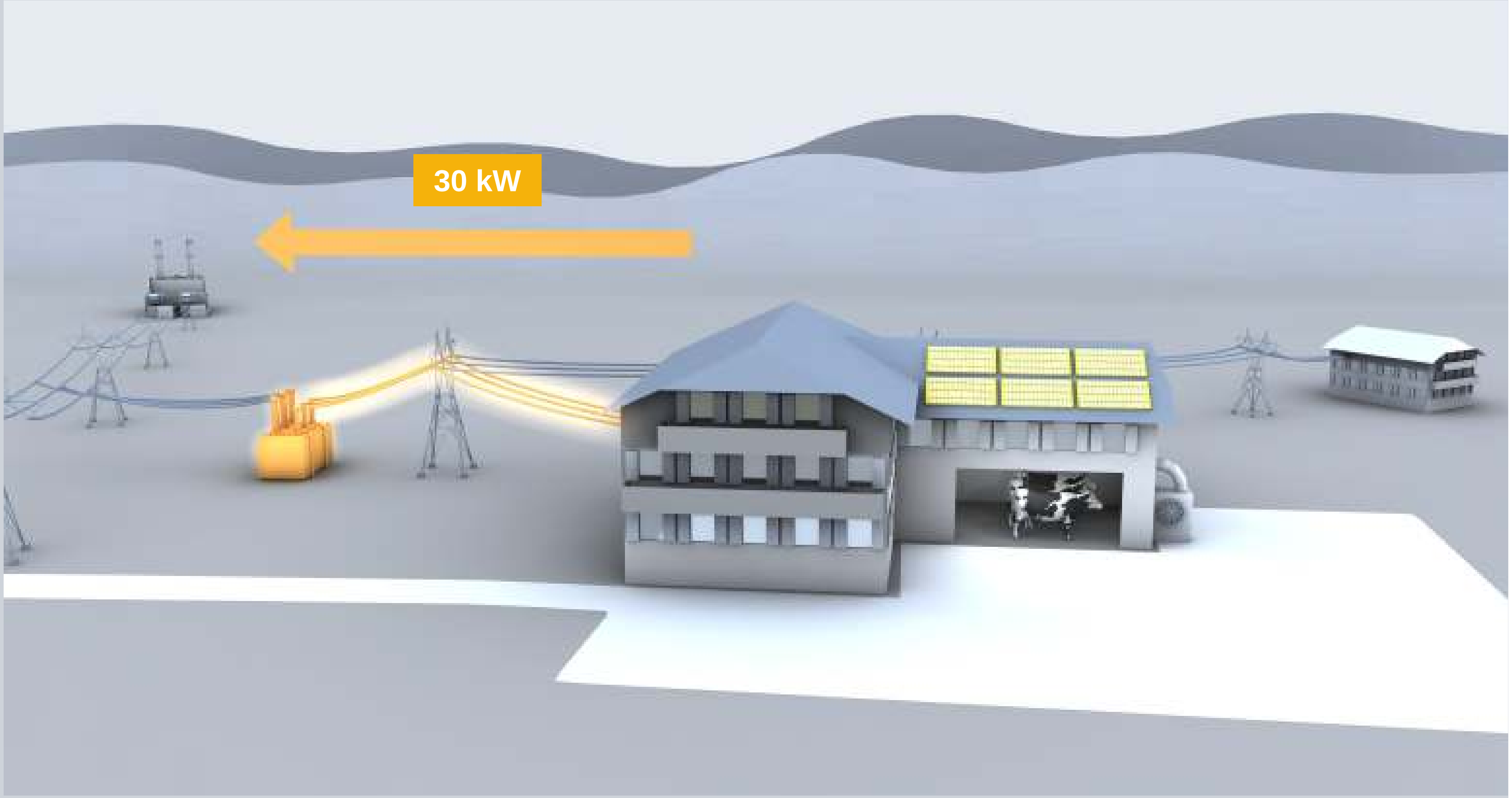
© Siemens AG, Corporate Technology

… a system with central generation and unidirectional power flow …



© Siemens AG, Corporate Technology

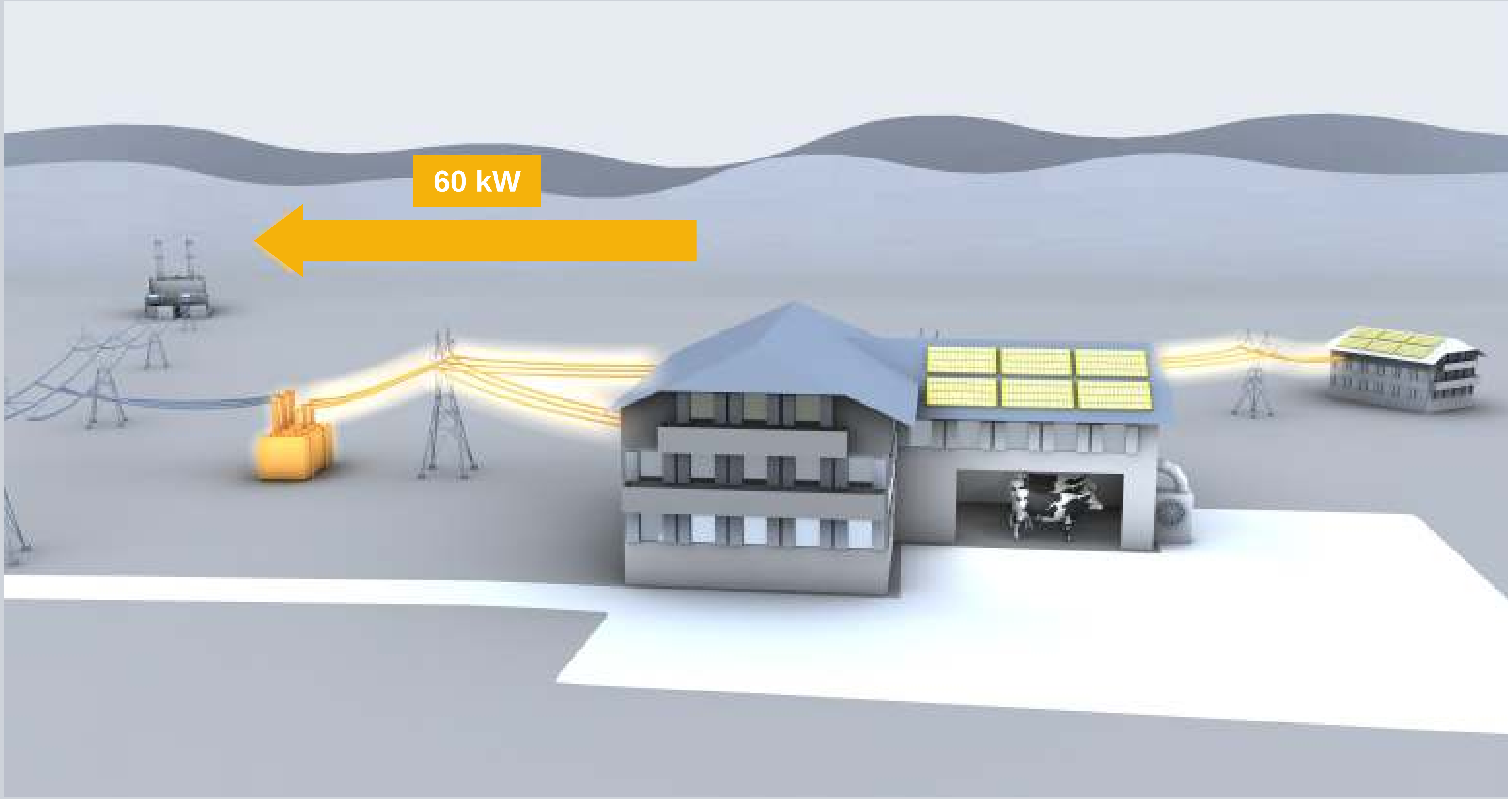
… is changing to decentralized generation



© Siemens AG, Corporate Technology

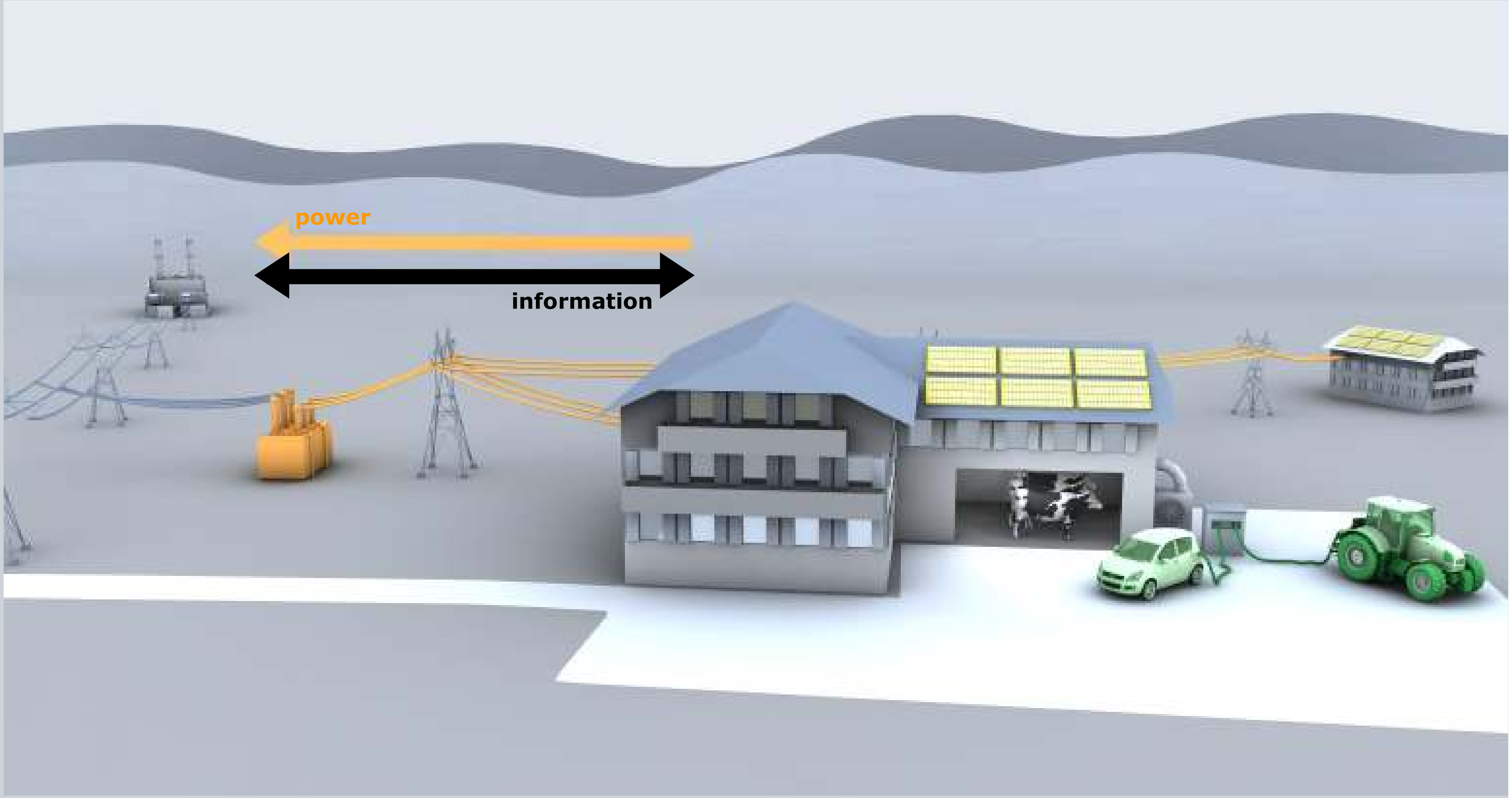
SIEMENS

… is changing to decentralized generation



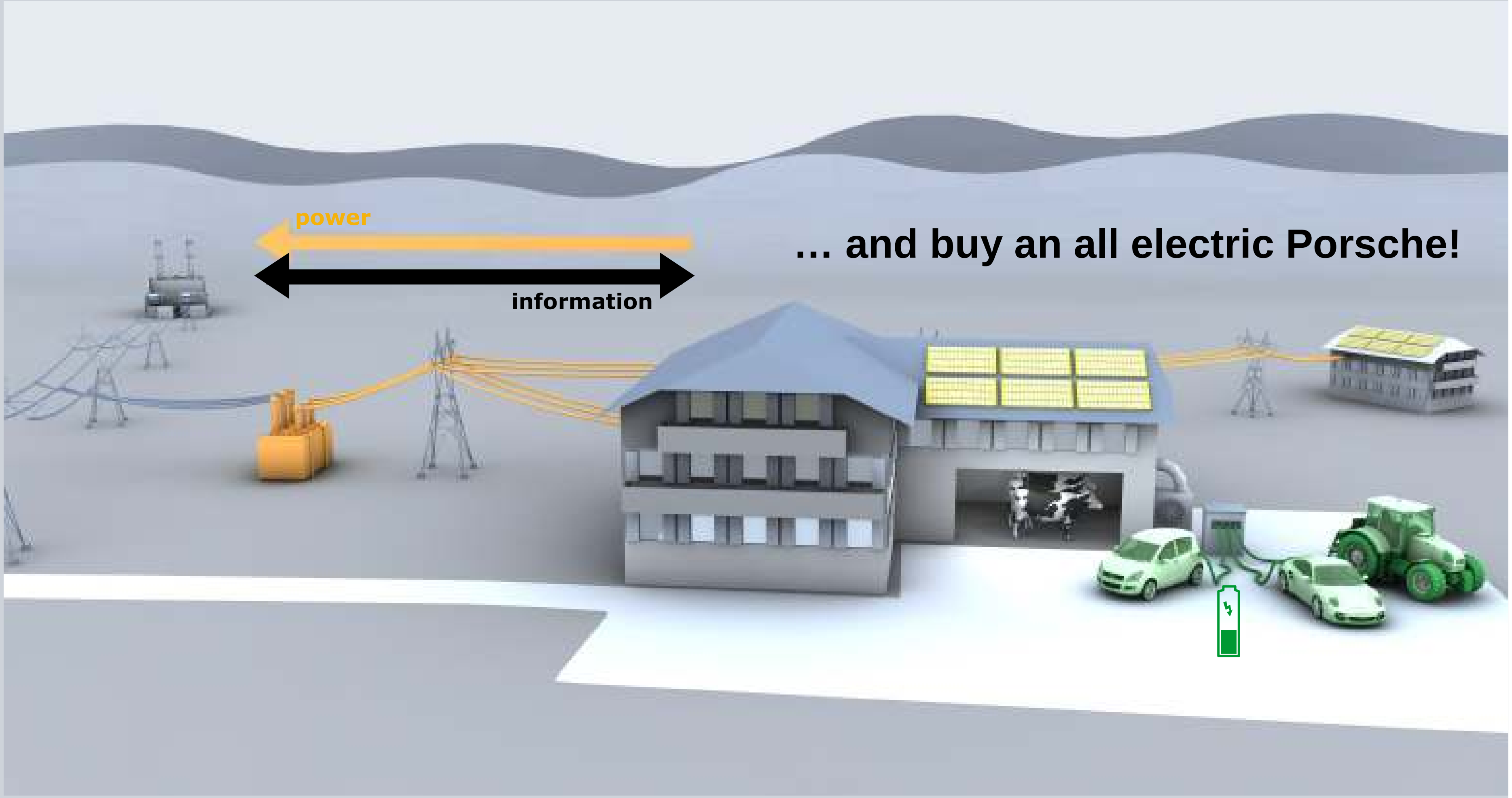
© Siemens AG, Corporate Technology

With innovative technology,
Consumers transform into real Prosumers …



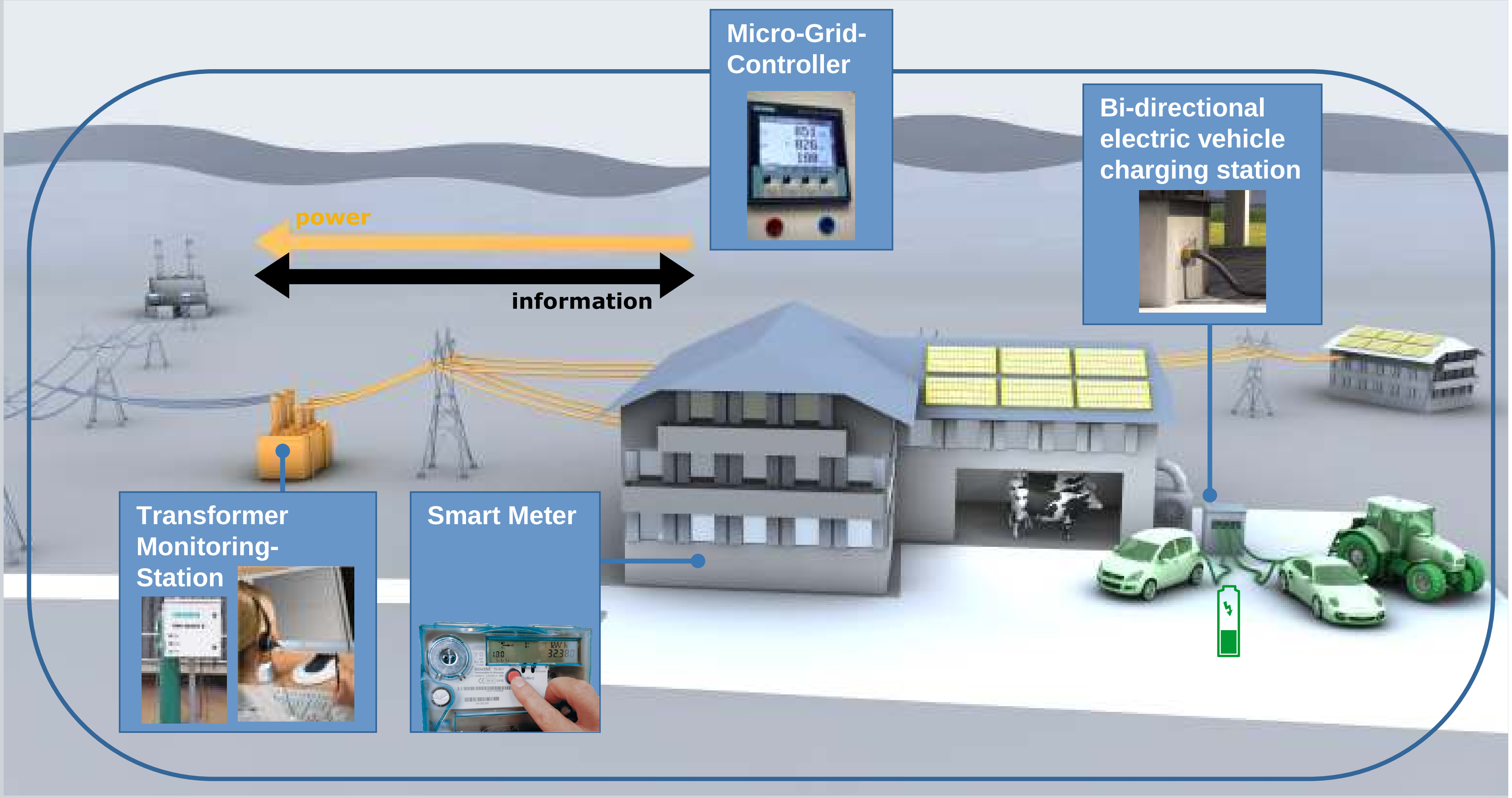
© Siemens AG, Corporate Technology

… trade power and earn money …



 © Siemens AG, Corporate Technology

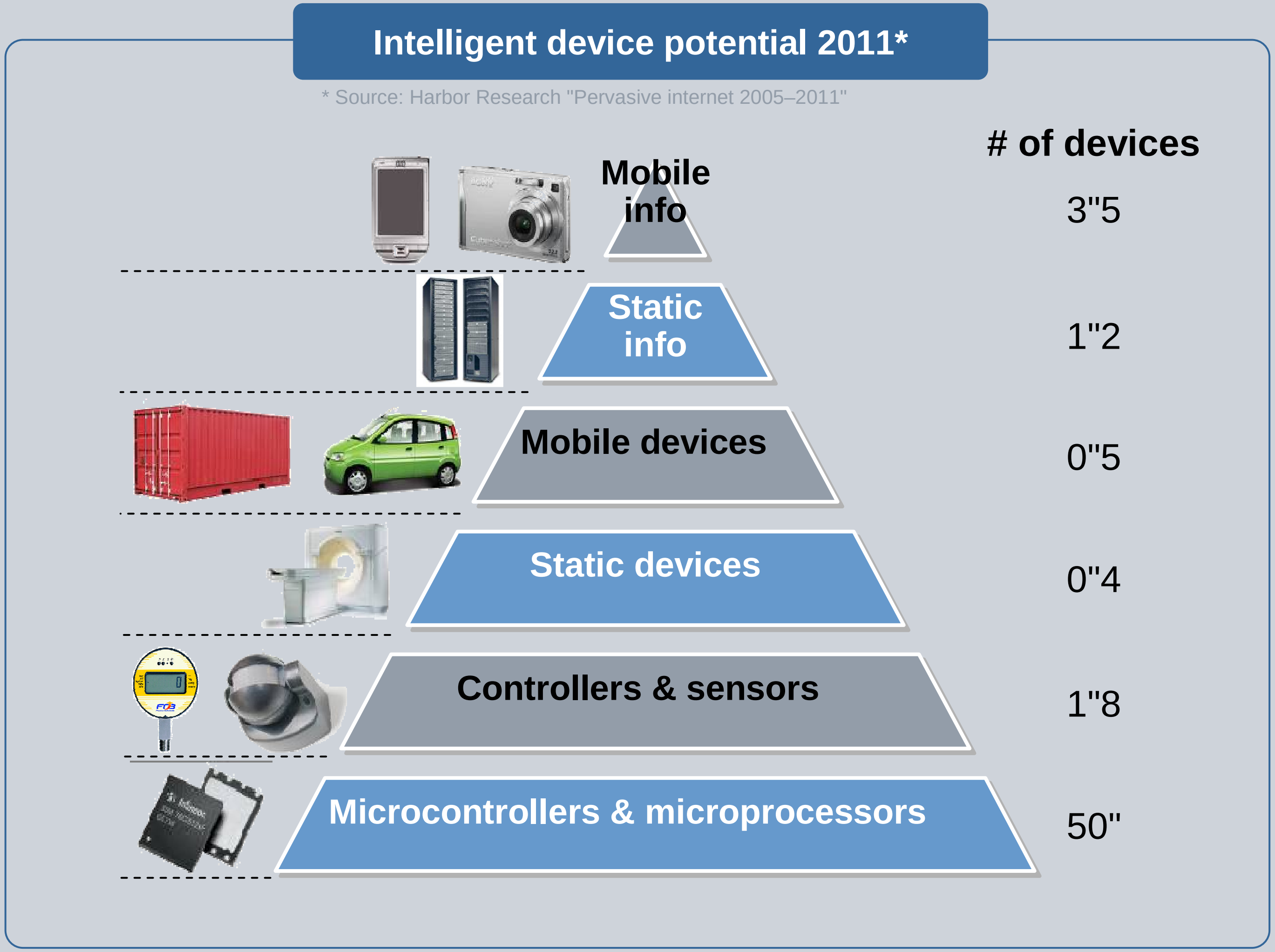
Intelligent components enable the transition from Conventional Grids to Smart Grids



 © Siemens AG, Corporate Technology

Observed Trend:
Increasing Intelligence and Open Communication

SIEMENS



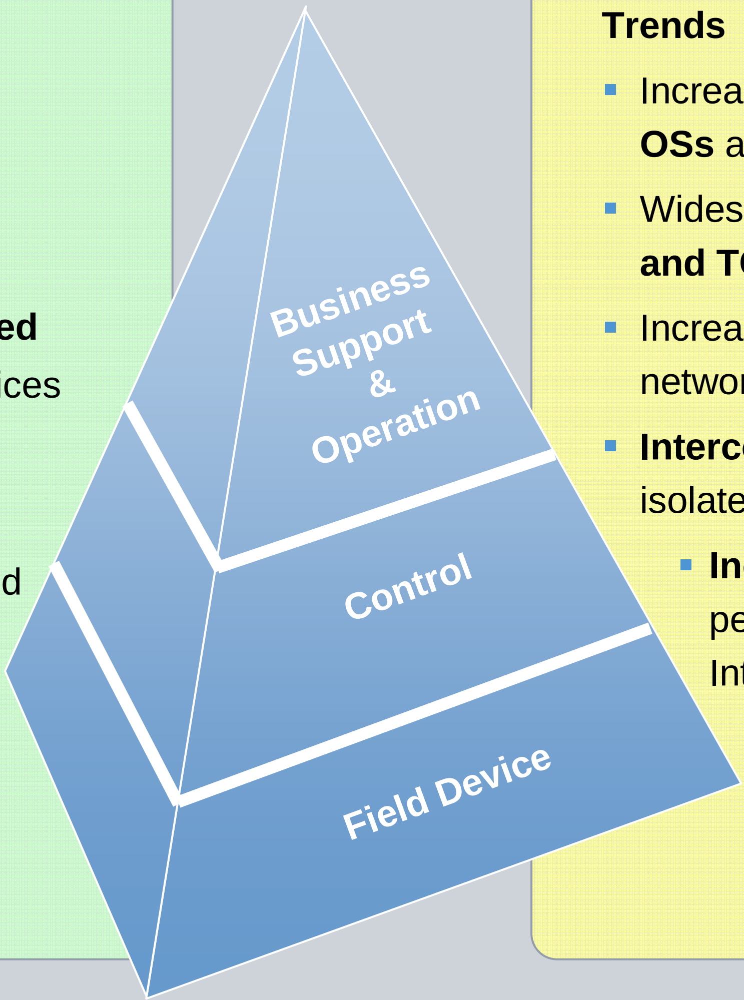
© Siemens AG, Corporate Technology

IT-Security Becomes a Pre-requisite for Future Control Systems Driven by Convergence of Safety & Security

SIEMENS

Current Situation

- Predominantly **isolated** communication networks
- Often **proprietary** networks and applications
- **(Limited) Physically secured** access to networks and devices
- **Long lifetime** of control equipment
- Systems are mainly designed for **performance, reliability and safety**, not security
- Often **availability** is the most important security objective



Trends

- Increasing **usage of standard OSs** and applications
- Widespread usage of **Ethernet and TCP/IP** (including Internet)
- Increasing usage of **wireless** networks
- **Interconnection** of formerly isolated networks
  - **Increasing intelligence** in peripheral components (e.g. Intelligent Access Devices)
    - **IT-security becomes a pre-requisite for safety applications**

 © Siemens AG, Corporate Technology

Smart Grid Scenarios – Incorporation of Decentralized Energy Resources and Flexible Loads requires Security

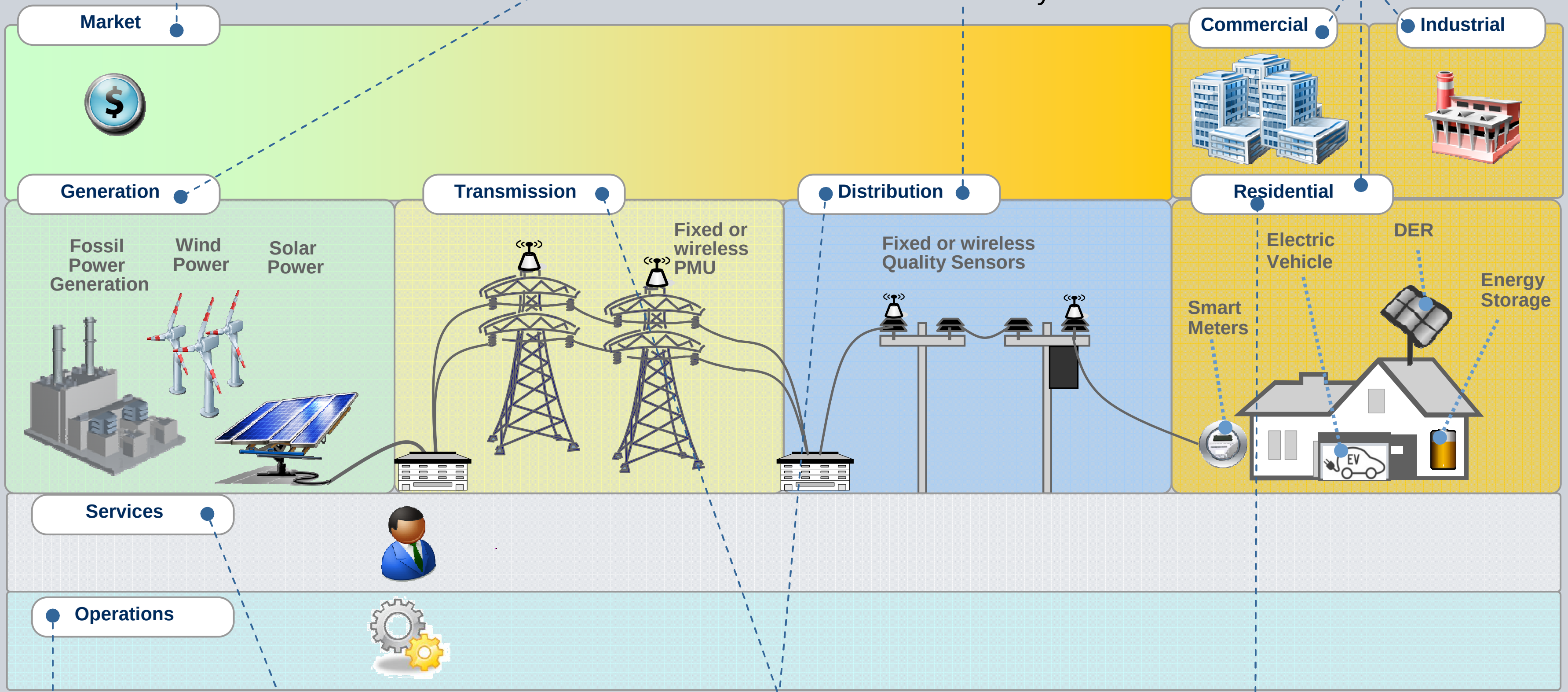
SIEMENS

- Automated billing
- Innovative pricing
- Market place interaction

- Fully integrated energy sources including renewables, biomass, etc.
- Load balancing

- Integration of DER
- Electro Mobility

- Demand response management
- Microgrids



- Remote energy management and control
- Load Monitoring and Balancing

- Real-time outage notification
- Power Quality Monitoring (e.g., through application of PMUs)

- Smart metering
- Smart appliances

 © Siemens AG, Corporate Technology

Typical Components for Smart Grid Interaction with Smart Homes

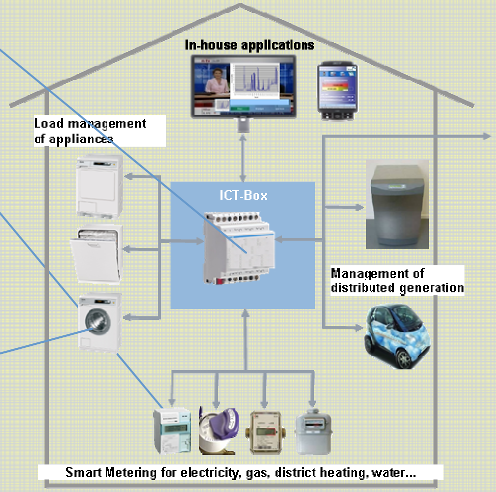
SIEMENS

Smart Energy Distribution

- **Control Center**
  - **Function**: Protection and control of the energy facilities
- **Substation Controller**
  - **Function**: Concentration of information for upper layers, protocol conversion
- **Protection Field Device**
  - **Function**: Protection of the energy facilities (e.g., switching of circuit-breaker)
- **Measurement Field Device – Phasor Measurement (PMU)**
  - **Function**: Measurement of phase angle (currents and voltages, phase difference by which the voltage leads or lags the current in an AC circuit) to provide information about power quality.

Smart Home

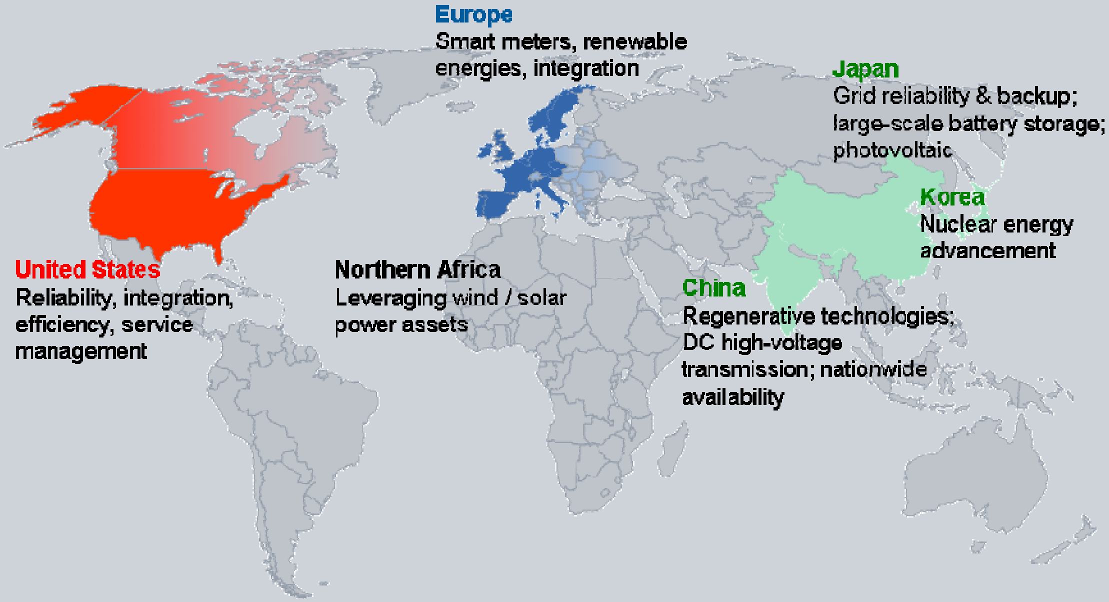
- **Home Energy Gateway**
  - **Function**: Provides home energy abstraction and remote access facilities for load balancing or remote administration
- **Measurement Field Device – Smart Meter**
  - **Function**: Measurement power consumption, e.g., in residential, commercial, or industrial use cases.
- **Smart Home Equipment**
  - **Function**: Allows intelligent control of energy consumption



© Siemens AG, Corporate Technology

Drivers for Smart Grid – Regional Differences and Consensus

SIEMENS



Regional differences

- Topics: Market communication, Metering, Home & Building, Demand Response, Electric Mobility, Security (privacy, etc.)
- Criteria: regulated
- Evidence: different standards referenced in studies and different national and regional regulation

Likely consensus

- Topics: Architecture, Communication, Common Data Models, DER, RES
- Criteria: Interoperability, non-regulated
- Evidence: Set of Core Standards (e.g. IEC TC 57) identified across studies

Information taken from original slide set from Status of activities Joint Working Group on standards for Smart Grids in Europe

 © Siemens AG, Corporate Technology

Core Standards for Smart Grids
IEC TC57 Reference Architecture

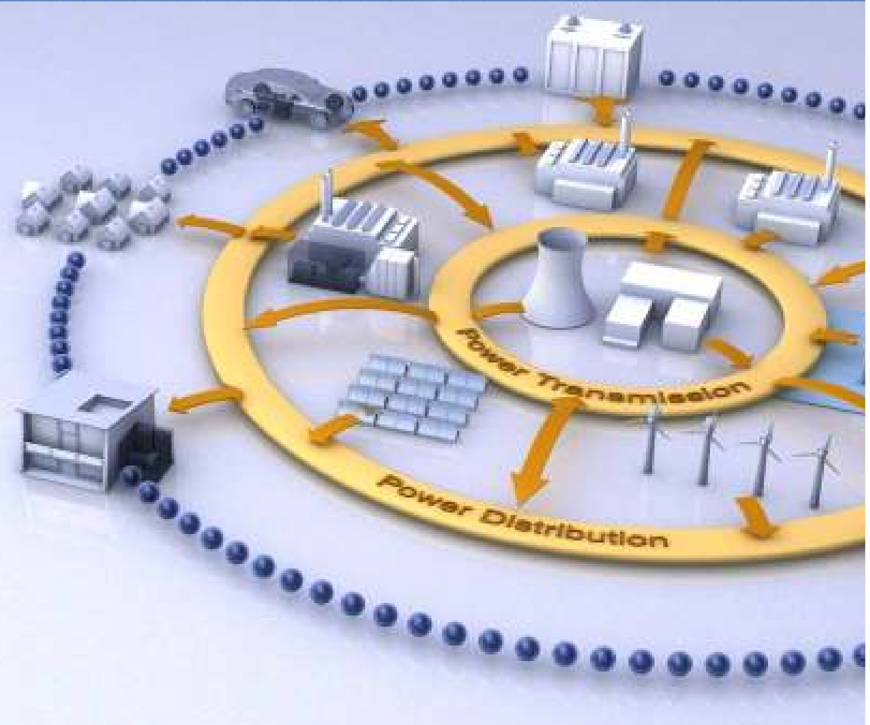
Common Information Model
IEC 61970 / 61968

Market Communication
IEC 62325

Substation Automation
Distribution Automation
DER Automation
IEC 61850

Tele-control Protocols
IEC 60870

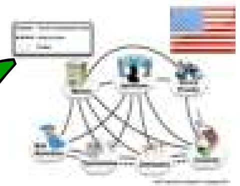
Smart Metering
IEC 61334 DLMS, IEC 62056 COSEM



Cyber Security
IEC 62351

IEC roadmap

Deutsche Normungsroadmap

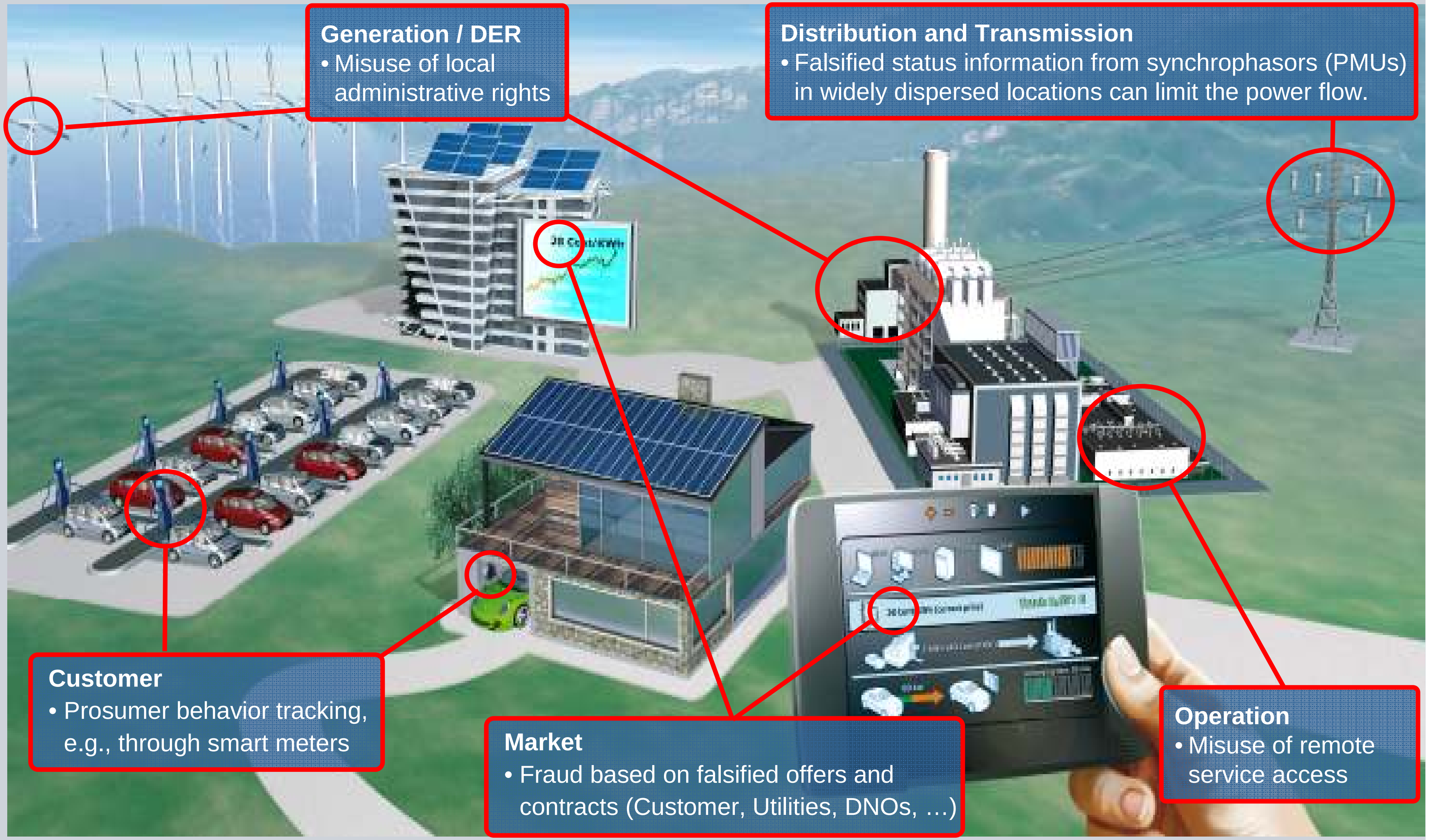


NIST
Interop Report

© Siemens AG, Corporate Technology

Security Requirements for Smart Grid Applications stem from a Variety of Potential Attacks (examples)

SIEMENS



 © Siemens AG, Corporate Technology

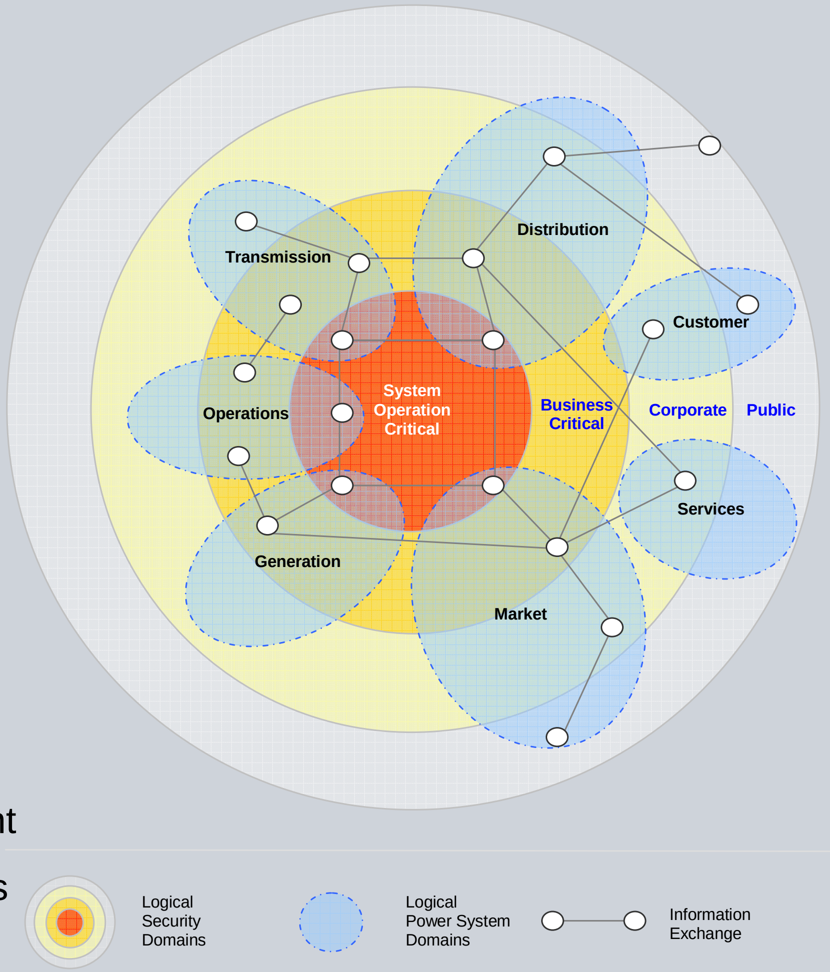
Smart Grid – (Some) Security Objectives

Generic objectives

- Availability and reliability of energy provisioning
- Limitation of attack effects (geographical and functional)
- Authorized control actions on smart grid components
- Correct billing of energy transactions between involved peers (prosumer, operator, market, energy provider)

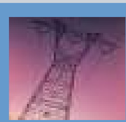
Additional scenario specific objectives

- Smart Grid/Smart Home Interactions:
  Privacy of metering information (Smart Metering)
- Smart Grid internal: Access to communicated and stored data only for authorized personnel („Keep outsiders out“)
- Smart Grid cross domain: Clearing of energy and payment transactions between energy providers, DNOs, microgrids with different level of trustworthiness



© Siemens AG, Corporate Technology

Energy Automation Systems vs. Office World
Management & Operational Characteristics

	Energy Control Systems 	Office IT 
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	Up to 20 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

© Siemens AG, Corporate Technology

Security Regulation/Standards/Guidelines ensure Reliable Operation of the Smart Grid (examples)

SIEMENS

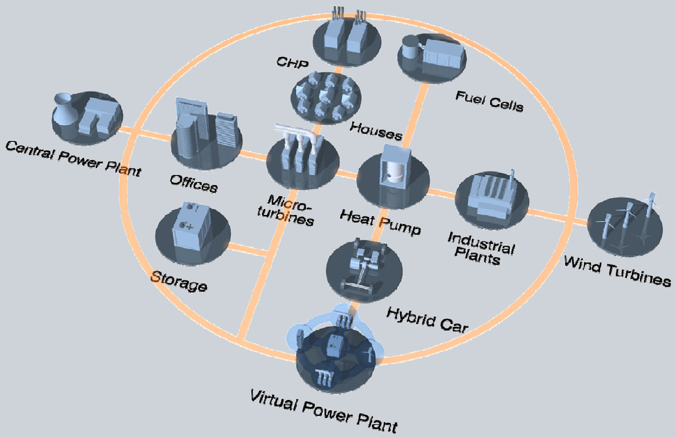
NERC – CIP | DoE ES-ISAC | AGA 12 | INL | EU JWG SG | BSI – BP

NIST – CSWG | CIGRE D2/B3 | BDEW – WP | VDEW | VDI/VDE 2182 | WIB

NIST – SP 800

DHS

ANSI



CERTs

DKE

CEN/CENELEC

FIPS 140 | DNP3 | W3C | OASIS | IEC 62443 | ETSI

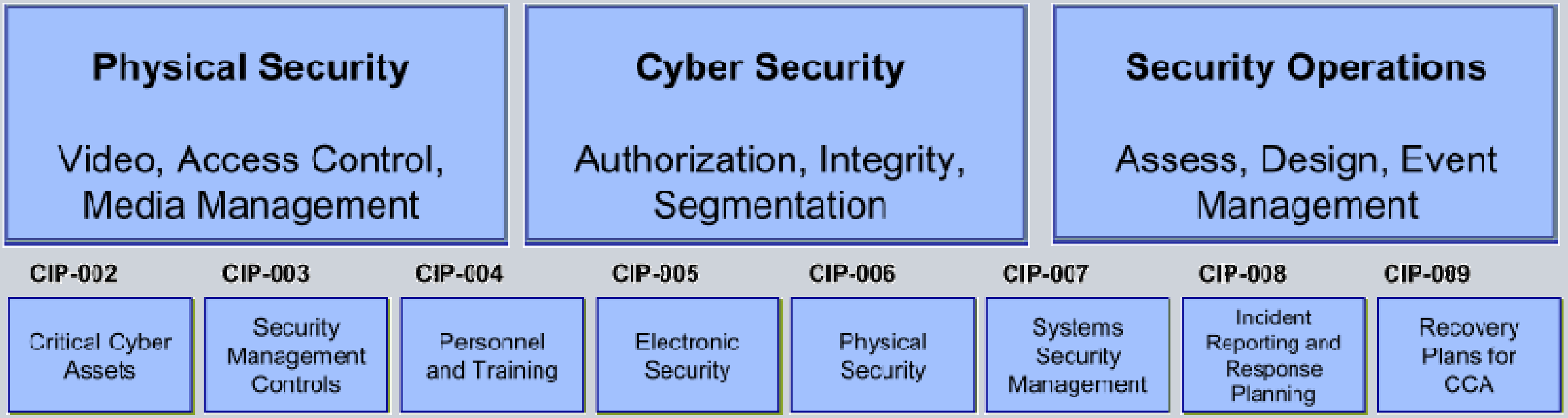
ISO 2700x | IEC 62351 | IEEE 1686 | IETF RFCs | ZigBee SEP | ISA 99

© Siemens AG, Corporate Technology

NERC CIP –
Critical Infrastructure Protection Standards

SIEMENS

- **North American Electric Reliability Corporation (NERC) = Non-Profit Organization in US, responsible for reliable power supply and coordination of North American energy networks**



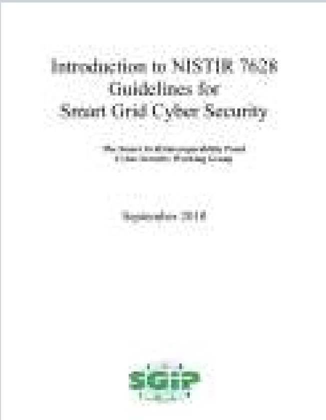
- **Binding for operators of power systems in USA, Canada and Mexico**
- **Unified format (intro, rules, measures, compliance (or deviation), regional specifics and history)**
- **Compliance process based on self audit, which must be repeated yearly**
- **Verification through a local NERC auditor, correction within 30 days required.**
- **CIP 010, 011 address “Bulk Electrical System Cyber System Categorization and Protection”**
  → new organization of existing requirements and elimination of non-routable protocol exception

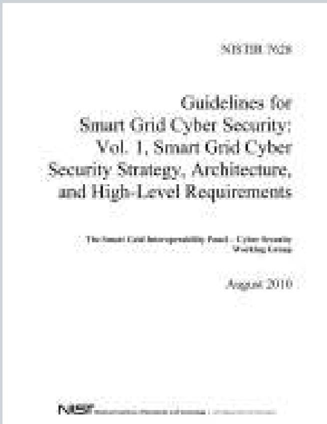
© Siemens AG, Corporate Technology

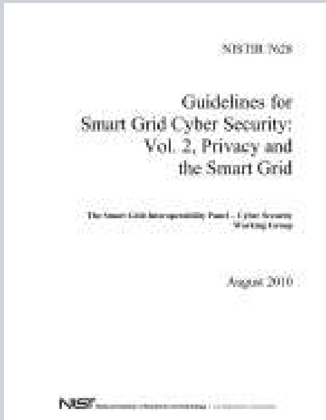
National Institute of Standards and Technologies – NIST Smart Grid Activities

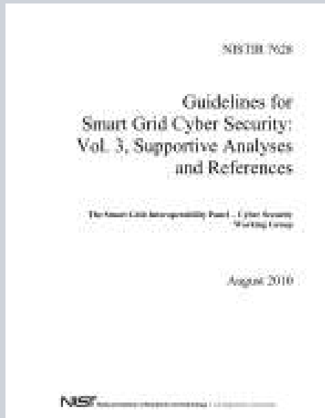
SIEMENS

- **Federal Technology Institution in the US. Activities established in 2009:**
- **Smart Grid Interoperability Panel (SGIP) fulfilling responsibilities under the 2007 Energy Independence and Security Act (members: commercial, scientific, public)**
- **Cyber Security Working Group (CSWG) under the umbrella of the SGIP with more than 500 members working in sub-groups including High Level Requirements, Vulnerabilities, Bottom-Up, Architecture, Standards Assessment, and Privacy**
- **CSWG published Interagency Report NIST IR 7628 (4 volumes)**
  - Supports development of an overall cyber security strategy for Smart Grid including risk mitigation
  - Include prevention, detection, response, and recovery


Introduction to NISTIR 7628
Guidelines for
Smart Grid Cyber Security


NISTIR 7628
Guidelines for
Smart Grid Cyber Security:
Vol. 1, Smart Grid Cyber
Security Strategy, Architecture,
and High-Level Requirements
August 2010

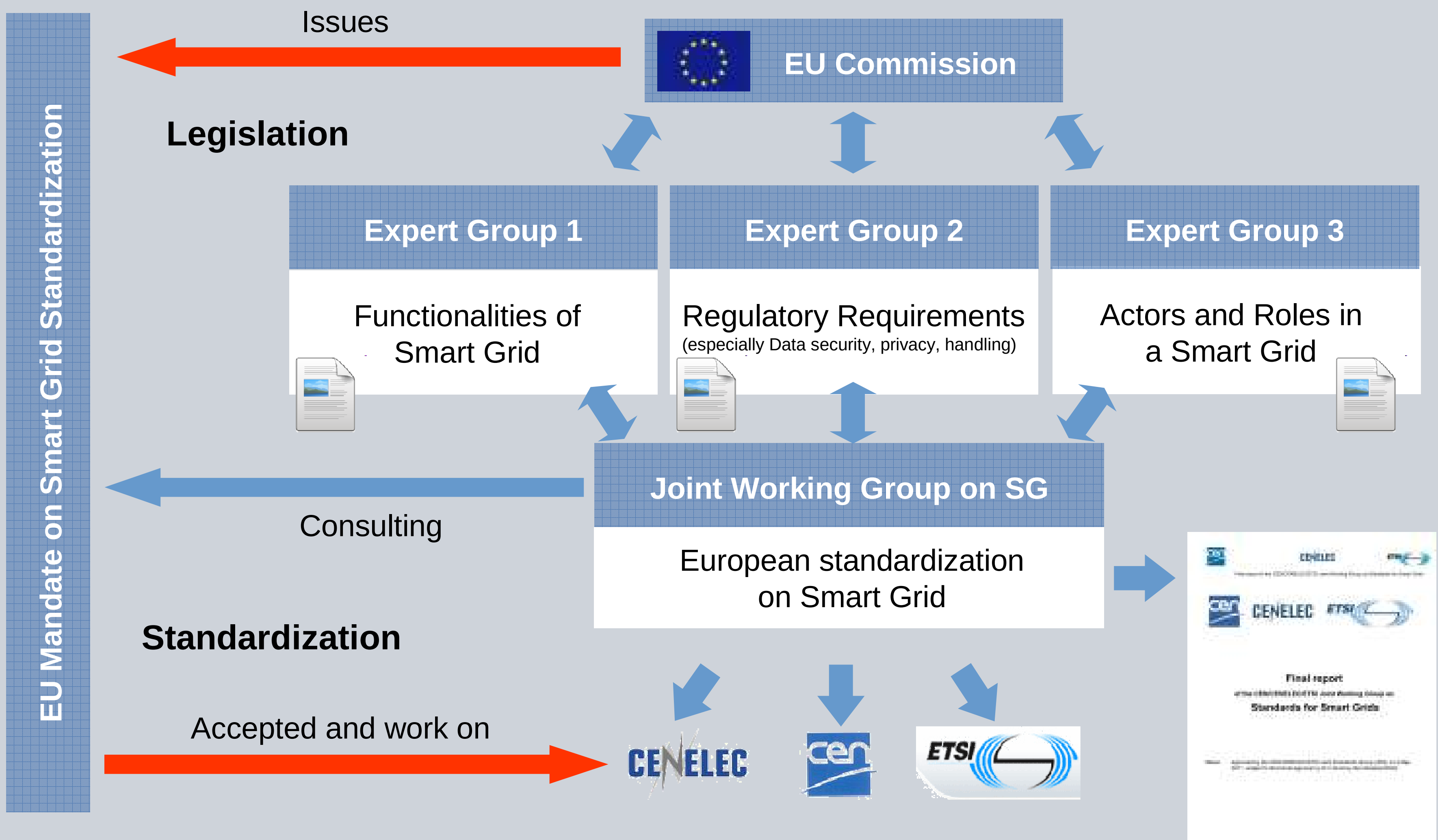

NISTIR 7628
Guidelines for
Smart Grid Cyber Security:
Vol. 2, Privacy and
the Smart Grid
August 2010


NISTIR 7628
Guidelines for
Smart Grid Cyber Security:
Vol. 3, Supportive Analyses
and References
August 2010

© Siemens AG, Corporate Technology

SIEMENS

Setup of Smart Grid Standardization in Europe



Information taken from original slide set from Status of activities Joint Working Group on standards for Smart Grids in Europe

© Siemens AG, Corporate Technology

EU Mandate M490 – Description of mandated work


Ref. Ares(2011)233514 - 02/03/2011

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY

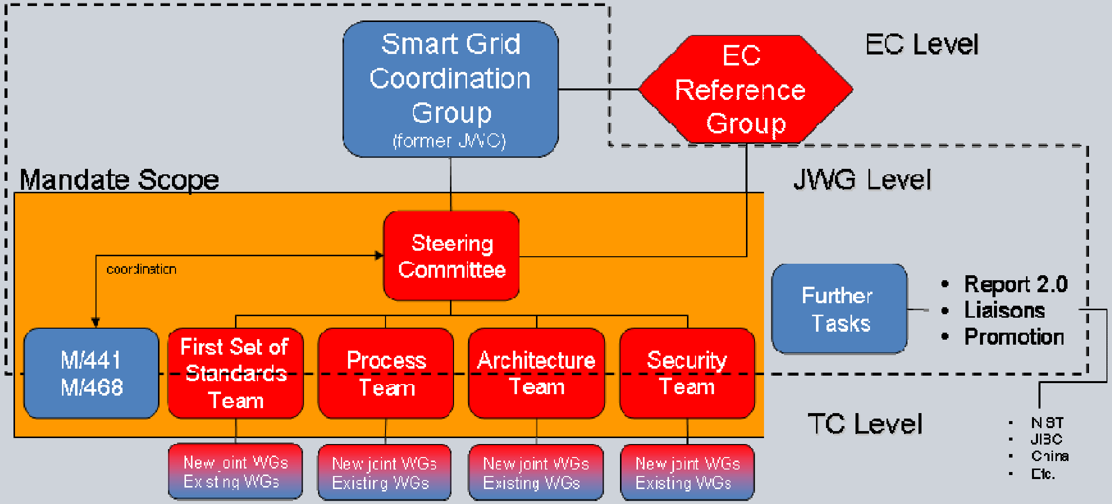
Directorate B - Security of supply, Energy markets & Networks
B.2 - Electricity & Gas

Brussels 1st March 2011
M/490 EN

Smart Grid Mandate

Standardization Mandate
to European Standardisation Organisations (ESOs) to support
European Smart Grid deployment

- **Technical Reference Architecture**
  Functional information data flows between the main domains and integration of systems and subsystems architectures
- **Set of Consistent Standards**
  Support information exchange (communication protocols and data models) and user integration into the electric system operation.
- **Sustainable standardization processes**
  and collaborative tools to enable stakeholder interactions, to improve and adapt to new requirements based on gap analysis.
- **Proposal of new structure:**



Information taken from original slide set from Status of activities Joint Working Group on standards for Smart Grids in Europe

© Siemens AG, Corporate Technology

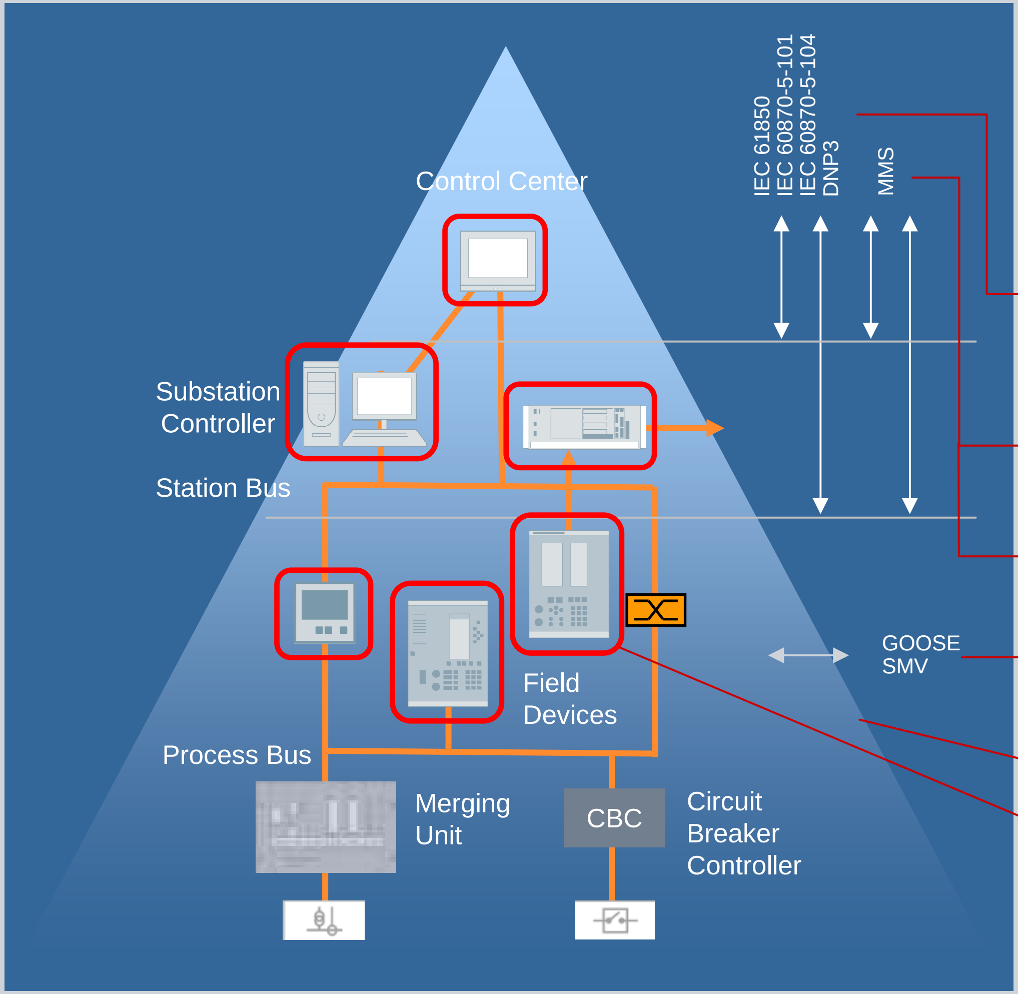
Security for Power System Control Networks
IEC TC57 WG15 – ISO/IEC 62351

- **Security services for Power System Control and Associated Communications**
- **IEC62351 is an umbrella standard consisting of several substandard targeting security features for dedicated communication scenarios focusing on**
  - **Integrity/Encryption** of data exchanged over networks using transport layer security 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
- **Responsible for maintaining and further evolving IEC 62351**
  - “Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series.”
  - “Undertake the development of standards and/or technical reports on end-to-end security issues.”

© Siemens AG, Corporate Technology

ISO/IEC 62351
Enabling secure modern energy control networks

SIEMENS



- **Integrity protection and encryption** of control data
- **Heavily uses asymmetric crypto** for authentication and authorization
- **Part 1**: Introduction
- **Part 2**: Glossary
- **Part 3**: Profiles including TCP/IP (cover those profiles used by ICCP, IEC 60870-5 Part 104, DNP 3 over TCP/IP, and IEC 61850 over TCP/IP)
- **Part 4**: Profiles including MMS (cover those profiles used by ICCP and IEC 61850)
- **Part 5**: Security for IEC 60870-5 and derivatives (covers both serial and networked profiles)
- **Part 6**: Security for IEC 61850 Peer-to-Peer Profiles (profiles that are not based on TCP/IP)
- **Part 7**: Network and System Management
- **Part 8:** Role Based Access Control
- **New Work Items**
  - Credential management (Part 9)
  - Security Architecture Guidelines (Report)

 © Siemens AG, Corporate Technology

Research Activities: Some Examples of Funded Projects addressing Security in the Smart Grid

SIEMENS

The following are just examples of projects addressing security explicitly.

There are certainly more.

EU funded

- FINSENY: Future Internet for Smart Energy
- OpenNode: Open Architecture for Secondary Nodes of the Electricity Smart Grid (http://www.opennode.eu/)

German (BMWi) funded (see also www.e-energy.de)

- E-DeMa: Development and demonstration of locally networked energy systems to the E-Energy marketplace of the future (http://www.e-dema.com/)
- Harz.EE.Mobility: Development and testing of ICT-based technologies for efficient introduction of electro mobility into the smart grid for grid integration of highly renewable power generation (https://www.harzee-mobility.de/)

© Siemens AG, Corporate Technology

Embedded Security Mechanisms Provide Essential Functionality for Ensuring System Integrity

SIEMENS

Security is required to ensure safety-relevant system properties in environments exposed to attacks

Substation Integrity Check	Verify integrity of overall substation installation (components, cabling, software). Ensures detection of unauthorized changes.
Original spare parts (Anti-Counterfeiting)	Ensure that original spare parts are installed, and not counterfeited replacements with poor quality.
Software Integrity Check	Ensure that firmware and configuration has not been altered. Device is going to regular operation only with valid configuration.
Secure Software Update	Ensure that only approved software updates are installed in compliance with defined update procedures.
Secured Machine Communication	Prevents manipulation and interception of machine control and service data when transmitted (device control, remote service).

© Siemens AG, Corporate Technology

Summary and Challenges

Summary

- Machine-2-Machine connectivity down to field devices is a major driver for the Smart Grid
- Security has been acknowledged as one of the important corner stones within a Smart Grid
- Technical security solutions for dedicated parts of the smart grid are provided through standards
- Regulation and guideline documents are available and are being further evolved
- Research is addressing smart grid security in several funded projects

Challenges

- Coordination and alignment of requirements from plurality of stakeholders (IT, Energy, Consumer, etc.)
- Coping with differences in innovation speed, e.g., Metering: Metrological data vs. Energy Management
- Political influence → Regulated markets; Mandates in Europe
- Device-oriented security and identity infrastructure (processes, scalability, limits of authority, …) supporting efficient creation, distribution and handling of cryptographic credentials
- Device security platform modules and their integration into products & production
- Security has to cope with domain specific characteristics (device capabilities, multicast, …)
- Migration from existing environment to an environment featuring appropriate IT security

© Siemens AG, Corporate Technology

Siemens Energy Sector –
Answers for energy supplies

SIEMENS

Energy products and solutions – in 6 Divisions

Oil & Gas	Fossil Power Generation	Renewable Energy	Energy Service	Power Transmission	Power Distribution






© Siemens AG, Corporate Technology