SMART GRID PROTECTION AGAINST CYBER ATTACKS

1st Stakeholder Enagement Workshop

Smart Grid Security Architectures and Standards

Graz, May 20th, 2014

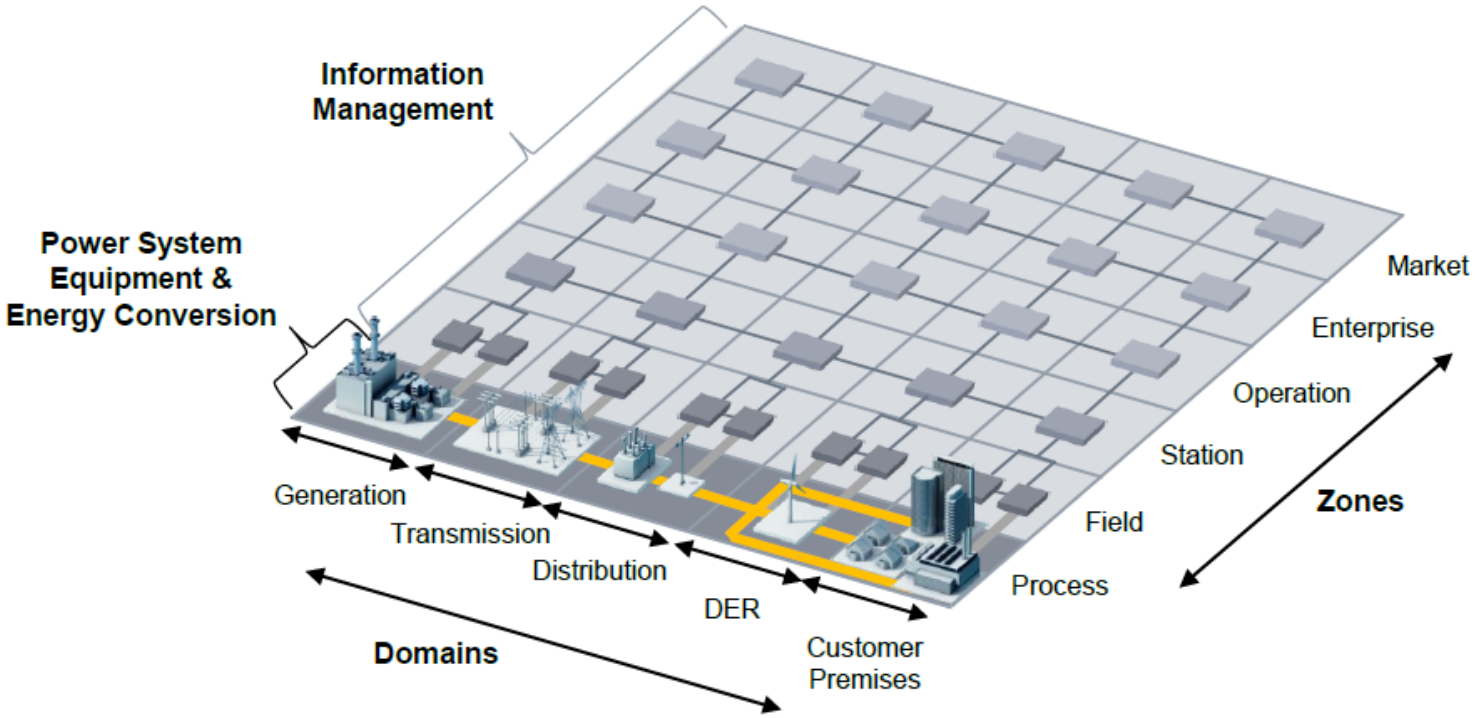
EU FP7 Programme Contract No. 608224

Smart Grid Reference Architecture

- "Fundamental **organisation of a system** embodied in its **components**, their **relationships** to each other and to the environment and the **principles guiding its design and evolution**" (IEEE-Std-1471-2000)
- Defines restrictions for a specific instantiation
- Benefits:
  - Facilitate information sharing between different stakeholders in pre-standardisation (e.g. research projects) and standardisation
  - Analysis of Smart Grids use cases via the SGAM methodology (facilitate analysis of different architectural alternatives & use case implementation)
  - Identify areas where appropriate standards are missing (via generic use cases)
  - …

Smart Grid Plane

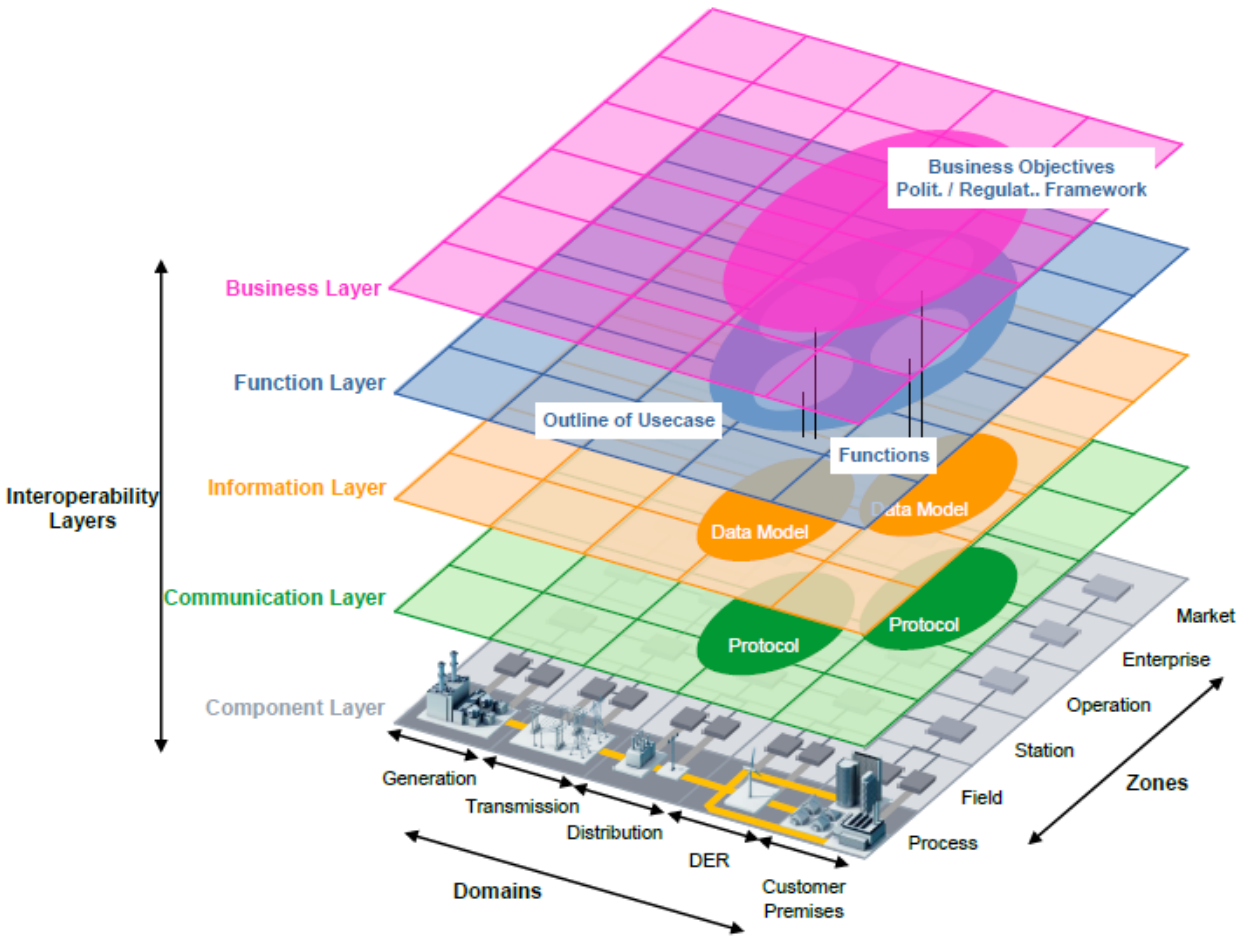
- Physical **Domains** of the electrical energy conversion chain
- Hierarchical **Zones** for power systems management



Source: CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, 2012.

EU FP7 Programme Contract No. 608224

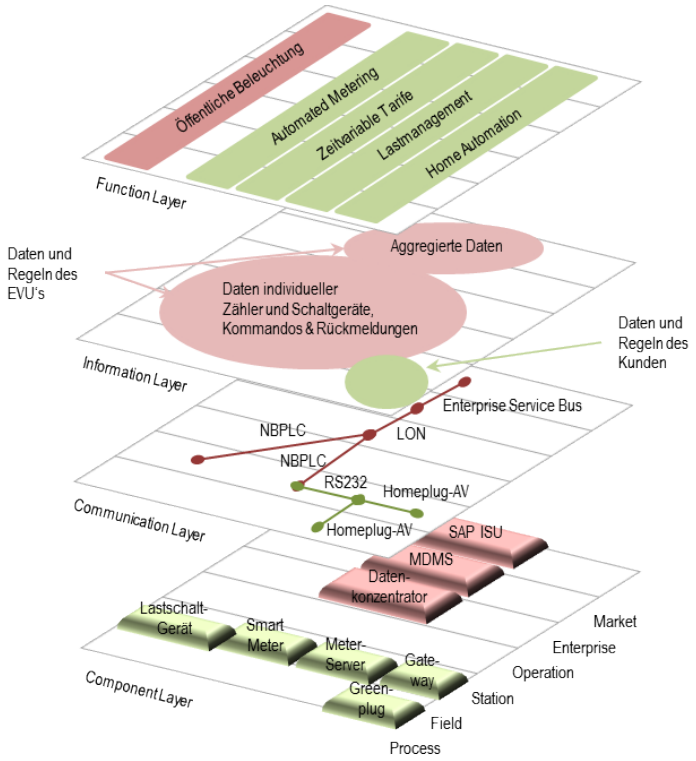
Smart Grid Architecture Model

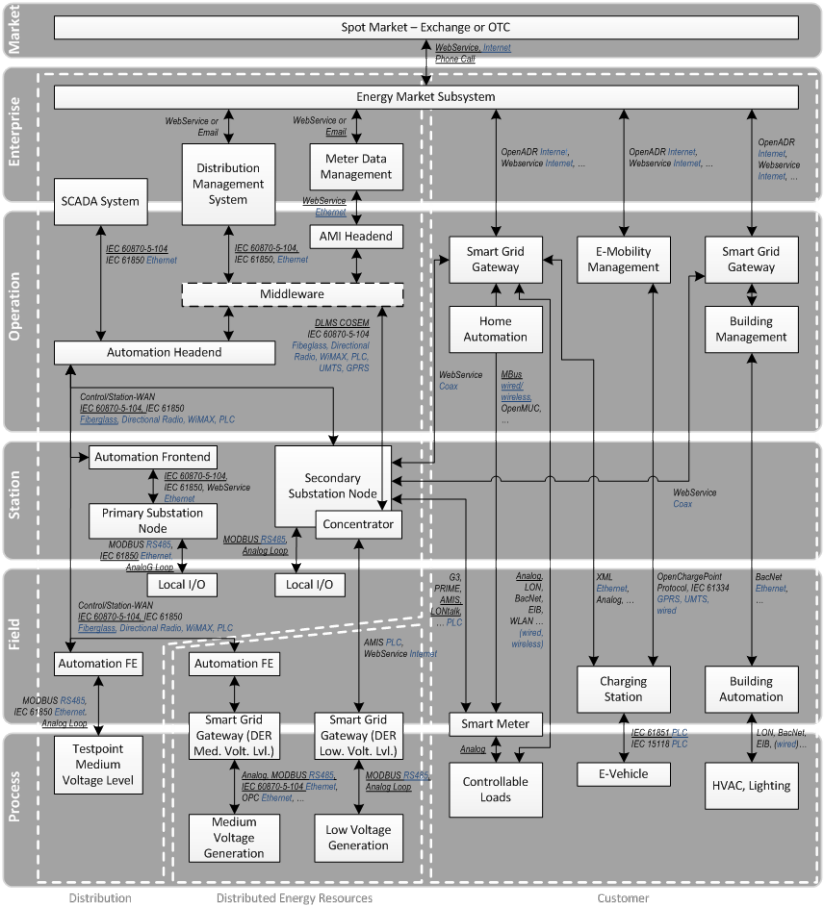


Source: CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture, 2012.

(SG)² approach

- Analyse relevant pilot projects & deployed system architectures and map them to SGAM





Smart Grid Security Standards

SMART GRID PROTECTION AGAINST CYBER ATTACKS

- **IEC 61850:** A set of standards describing the design of electrical substation automation and distributed energy resources
- **IEC 60870-5**: Series of standards used for SCADA system to RTU data communications in EU
- **IEC 62351**: Security measures for TC 57 series of protocols, including authenticated access & data transfer, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection
- **IEC 62443**: Network and system security in industrial communication networks
- **ENISA:** Appropriate security measures for Smart Grids, Smart Grid Threat Landscape, …
- **NIST IR 7628** Guidelines for Smart Grid Cyber Security
- ISO 27k, BSI Protection Profiles & Baseline Protection Catalogues, …

EU FP7 Programme Contract No. 608224

SPARKS objectives

- **Identify baseline Smart Grid reference architectures:**
  - Based on existing architectures, frameworks and projects
  - Identify required changes, enhancements or extensions
- **Provide security guidance:**
  - Based on existing metrics, standards, guidelines, and best practices (e.g., from past projects)
  - Example: Smart grid resilience management patterns: reusable descriptions of known-good strategies for addressing a specific challenge
- **Define Smart Grid security standards recommendations:**
  - Related both to Smart Grid security architecture and to real-time monitoring tools and services that should be addressed within new or existing standards

Questions

- Which standards do you consider help make the smart grid more secure?
  - For example IEC 62351, NIST 7628, BSI ...
- Which standards are relevant to your operations? Do you actively track these?
  - For marketing
  - For compliance (please state relevant regulation)
  - For creation of defences
  - For auditing suppliers
- Do you perceive any gaps in the various cyber security standards?
  - Gaps in existing standards?
  - Security-related areas which require standards?
- Are standard reference architectures relevant to your operations? Which ones?
  - For example SGAM, TOGAF, ...?
- Do you participate in any organizations/working groups defining these standards/architectures?
  - At the national level
  - At the international level