Smart TSO-DSO interaction schemes, market architectures and ICT Solutions for the integration of ancillary services from demand side management and distributed generation

ICT requirements specifications

D3.1

Authors:

R. Rodríguez, K. Bañuelos, J.A. López, A. Gil de Muro, K. Mendibil (TECNALIA), S. Horsmanheimo, H. Kokkoniemi-Tarkkanen, L. Tuomimäki (VTT), K. N. Gregertsen, I.C.R. Tardy (SINTEF ICT), D. Ectors (VITO), C. A. Andersen (EURISCO), F. Andren-Pröstl, M. Faschang, F. Lehfuss, M. Stefan, F. Kupzog, T. Strasser (AIT), C. Arrigoni, F. Zanellini (SIEMENS), M. Esser (VODAFONE), D. Moneta (RSE), M. Baldini, S. Bruschi (SELNET/EDYNA)

Distribution Level	Public
Responsible Partner	17 - TECNALIA
Checked by WP leader [name surname]	Date: 04/10/2016 Seppo Horsmanheimo (VTT)
Verified by the appointed Reviewers [name surname, name surname]	Date: 11/11/2016 Loui Algren (Energinet.dk) Eric Estrade (Vodafone Group)
Approved by Project Coordinator	Date: 18/11/2016 Gianluigi Migliavacca (RSE)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 691405

Issue Record

Planned delivery date	31/08/2016
Actual date of delivery	30/11/2016
Status and version	Final Draft

Version	Date	Author(s)	Notes
0.1	03/06/2016	TECNALIA and all task participants	First draft
1	15/07/2016	TECNALIA	Second draft after comments from task participants
2	23/09/2016	TECNALIA	Document reworked following coordinator's input on previous version and new inputs of other project tasks
2.1	04/10/2016	TECNALIA	Comments from task partners included: EURISCO, SINTEF, TECNALIA, VITO, VODAFONE, VTT. Introduction, conclusions and executive summary added.
2.2	10/10/2016	TECNALIA	General comments from coordinator affecting section 2
2.3	18/11/2016	TECNALIA	Comments from reviewers (Energinet.dk and Vodafone) and coordinator included.

About SmartNet

The project SmartNet (http://smartnet-project.eu) aims at providing architectures for optimized interaction between TSOs and DSOs in managing the exchange of information for monitoring, acquiring and operating ancillary services (frequency control, frequency restoration, congestion management and voltage regulation) both at local and national level, taking into account the European context. Local needs for ancillary services in distribution systems should be able to co-exist with system needs for balancing and congestion management. Resources located in distribution systems, like demand side management and distributed generation, are supposed to participate to the provision of ancillary services both locally and for the entire power system in the context of competitive ancillary services markets.

Within SmartNet, answers are sought for to the following questions:

- Which ancillary services could be provided from distribution grid level to the whole power system?
- How should the coordination between TSOs and DSOs be organized to optimize the processes of procurement and activation of flexibility by system operators?
- How should the architectures of the real time markets (in particular the markets for frequency restoration and congestion management) be consequently revised?
- What information has to be exchanged between system operators and how should the communication (ICT) be organized to guarantee observability and control of distributed generation, flexible demand and storage systems?

The objective is to develop an ad hoc simulation platform able to model physical network, market and ICT in order to analyse three national cases (Italy, Denmark, Spain). Different TSO-DSO coordination schemes are compared with reference to three selected national cases (Italian, Danish, Spanish).

The simulation platform is then scaled up to a full replica lab, where the performance of real controller devices is tested.

In addition, three physical pilots are developed for the same national cases testing specific technological solutions regarding:

- monitoring of generators in distribution networks while enabling them to participate to frequency and voltage regulation,
- capability of flexible demand to provide ancillary services for the system (thermal inertia of indoor swimming pools, distributed storage of base stations for telecommunication).

Partners

Table of Contents

List of Abbreviations and Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
AC	Alternating Current
ACL	Access Control List
ACSI	Abstract Communication Service Interface
ADMS	Advanced DMS
ADR	Automated Demand Response
AIT	Austrian Institute of Technology
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
API	Application Programme Interface
APN	Access Point Name
AS	Ancillary Service
ASDU	Application Service Data Units
ASN.1	Abstract Syntax Notation One
BACS	Building Automation and Controls System
CCS	Combo Charging System
CEM	Customer Energy Management (System)
CIM	Common Information Model
CIS	Customer Information System
COSEM	Companion Specification for Energy Metering
CMP	Commercial Market Player
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CS	Coordination Scheme
CSD	Circuit Switched Data
CSO	Charging Service Operator
CSEP	Consortium for SEP 2.0 Interoperability
CSP	Customer Service Profile
cVPP	Commercial VPP
DDE	Designated Dispatch Entity (EI)
DG	Directorate-General (EC)
DG	Distributed Generation
DER	Distributed Energy Resource
DLMS	Device Language Message Specification (originally Distribution Line Message Specification)

DMS	Distribution Management System
DR	Demand Response
DSL	Digital Subscriber Line
DSM	Demand Side Management
DSO	Distribution System Operator
EA	Enterprise Architect (software)
EC	European Commission
ECAN	ENTSO-E Capacity Allocation and Nomination System
EDI	Electronic Data Interchange (EDI)
EDM	Energy Data Management
EI	Energy Interoperation
EMG	Energy Management Gateway
EMM	ENTSO-E Modelling Methodology
EMS	Energy Management System
ENISA	European Union Agency for Network and Information Security
ENTSO-E	European Network of TSOs for Electricity
EPA	Enhanced Performance Architecture
ERP	Enterprise Resource Planning
ERRP	ENTSO-E Reserve Resource Process
ESI	Energy Services Interface
ESMP	European Style Market Profile
ESP	ENTSO-E Settlement Process
ESS	ENTSO-E Scheduling System
ETSO	European TSOs
EU	European Union
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
EXI	Efficient XML interchange
FACTS	Flexible AC Transmission System
FCR	Frequency Containment Reserve
FEP	Front End Processor
FRR	(SmartNet) Frequency Restoration Reserve (FRRs)
FRRa	Automatic Frequency Restoration Reserve
FRRs	SmartNet Frequency Restoration Reserve (FRR)
GIS	Geographic Information System
GOOSE	Generic Object Oriented Substation Events
GPRS	General Packet Radio Service
GSM	Global System for Mobile

HAN	Home Area Network
HBES	Home and Building Electronic System
HDLC	High Level Data Link Control
HES	Head End System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HV	High Voltage
HVDC	HV Direct Current
HVRS	HV Regulation System
ICCP	Inter-Control Centre Protocol
ICT	Information and Communication Technology
ID	Identification
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMO	Independent Market Operator
I/O	In/Out
IoT	Internet of Things
IP	Internet Protocol
IRM	Interface Reference Model
IS	International Standard
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
JMS	Java Message Service
LAN	Local Area Network
LN	Logical Node
LNAP	Local Network Access Point
LPWAN	Low Power WAN
LR-WPAN	Low-Rate Wireless Personal Area Network
LTE	Long Term Evolution
LV	Low Voltage
M2M	Machine-to-Machine
MAC	Media Access Control
MADES	Market Data Exchange Standard
MDM	Metering Data Management
MMS	Manufacturing Message Specification

MPLS	Multiprotocol Label Switching
MTC	Machine Type Communication
MV	Medium Voltage
MVRS	MV Regulation System
NB-IoT	Narrow Band IoT
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
NNAP	Neighbourhood Network Access Point
NNI	Network to Network Interface
NTP	Network Time Protocol
OBIS	Object Identification System
OCPP	Open Charge Point Protocol
OIM	Object Information Model
OMS	Outage Management System
OSI	Open System Interconnection
p	Active Power
P	Protocol
PDU	Protocol Data Unit
PEM	Privacy-Enhanced Electronic Mail
PHY	Physical Layer
PKI	Public Key Infrastructure
PLC	Power Line Communication
PLMN	Public Land Mobile Network
PMU	Phasor Measurement Unit
PRIME	PoweRline Intelligent Metering Evolution
PV	Photovoltaic
PWM	Pulse Width Modulation
Q	Reactive Power
QoS	Quality of Service
RDF	Resource Description Framework
RES	Renewable Energy Source
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request For Comments
RTU	Remote Terminal Unit
SAP	Service Access Point
Sc.	Scenario
SCADA	Supervisory Control and Data Acquisition

SCSM	Specific Communication Service Mapping
SEP	Smart Energy Profile
SGAM	Smart Grid Architecture Model
SG-CG	Smart Grid Coordination Group
SGIS	Smart Grid Information Security
SHIP	Smart Home IP
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SMS	Short Message Service
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToU	Time of Use (tariff)
TS	Technical Specification
TSO	Transmission System Operator
TT	Transfer Time
TV	Television
tVVP	Technical VPP
UC	Use Case
UCTE	Union for the Coordination of the Transmission of Electricity
UDP	User Datagram Protocol
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USEF	Universal Smart Energy Framework Foundation
UTC	Coordinated Universal Time
UTRAN	Universal Terrestrial Radio Access Network
VAR	Volt Ampere Reactive - measurement unit
VDSL	Very-high-bit-rate DSL
VEN	Virtual End Node (EI)
VPN	Virtual Private Network
VPP	Virtual Power Plant
VTN	Virtual Top Node (EI)
WADL	Web Application Descriptive Language
WAMPAC	Wide Area Measurement Protection and Control System (Wide Area Monitoring System)

WAN	Wide Area Network
WG	Working Group
WSDL	Web Service Description Language
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XSD	XML Schema Definition

Executive Summary

This report summarizes the core ICT requirements and their role in the TSO-DSO coordination schemes as identified by the project SmartNet (see D1.3 report "Basic models for TSO-DSO coordination) by breaking down the relationships between energy and communications up to describing physical communication components and interfaces. The interactions between stakeholders were also analysed in order to discover and classify the critical requirements for e.g. networking, security, latency, and data protocols for each TSO-DSO coordination scheme and use case.

This deliverable is written by industrial and academic partners to address both research and business oriented challenges. The goal was to capture and prioritize the communication requirements for today's and tomorrow's systems by utilizing project partners' competence in both energy and telecom domains.

This report is the foundation for the ICT architecture design work that will be analysed later in D3.2, where the captured requirements are converted into ICT specifications. This report focuses on business and function layers in the SGAM model whereas the D3.2 will concentrate on information, communication, and components layers. The outcome of this report is handed over to other project tasks in order to offer recommendations for ICT related issues.

After the introduction, **section 2** of the document sums up the **project approach**. Coordination schemes, use cases and market design are described to present the existing background, which is analysed in detail in section 4 to capture related ICT requirements.

In **chapter 3**, the high level framework of requirements coming from the **smart grids** strategy at European level is considered. The Smart Grid Coordination Group (SG-CG) has published several references that should be considered within SmartNet: the SGAM reference architecture permits a coordinated analysis of use cases; the communication and information set of standards proposed by the SG-CG should be taken as reference for the ICT architecture design; and the security aspects should also be observed.

In the **Annexes** (sections 9, 10, 11 and 12), EU level **ICT requirements for smart grids** are summarized looking at communication, information, security and component aspects. While chapter 3 focuses on the AS market requirements, annexes provide a broader perspective that can be used as reference for ICT solutions in other project tasks.

The following conclusions are derived from this section of the document:

- The **types of network** more directly linked to AS market processes are "Intra data-centre" networks, for communications between different applications within the same company or group of companies; and "backbone networks" for communications between different actors.
- In principle, market processes would require transfer times lower than 10 seconds. This is not a time critical functionality and most of the current **communication technologies** are able to meet this requirement: Ethernet, IP, fiber optic communications, DSL, web services and 3G/4G/5G.
- Market related **information standards** are already available. The main reference is IEC 62325. This standard, together with the ENTSO-E library EDI, already provides data models that can be used as reference for the interaction with energy market platforms.
- Since the impact of market related exchanges on network operation processes is not direct, **security** risks are "limited" regarding reliability, however data integrity issues should be also considered. Reference standards are the IEC 62351 and the IEC 27019 TR.

Section 4, as mentioned above, analyses in detail the coordination schemes, use cases and SmartNet market characteristics in order to extract ICT requirements from them. The **coordination schemes** clarify the communication links between actors. Business actors, business goals, business use cases and high level use cases are put into relationship to describe the business cases associated with each coordination scheme.

The **use cases** defined in the project framework, seven in total to describe 3 ancillary services, have been integrated into one consisting in four processes: pre-qualification, procurement, activation and settlement. This generic use case is described through scenario steps, and each of the steps defines an interaction between system actors (linked to business actors). From these interactions, the type of message to be exchanged is identified.

Market design establishes general ICT requirements dealing with:

- **Pricing**: locational information must be included in bids.
- **Bidding**: bid types and data models are provided.
- **Timing**: the clearing frequency, e.g. 5 minutes, sets a time limit requirement for all communications and computational steps to be performed within each market session (procurement and activation processes are involved).
- **Clearing**: SmartNet market algorithm considers both economic and technical constraints as input.

Chapter 5 of the document focuses on **project pilots**. ICT implications of pilots are captured and compared to those of the SmartNet approach. First, relevant interfaces between actors are obtained from pilot descriptions, and communication and information characteristics are extracted for each of them. In second place, pilot ICT characteristics reviewed to find how they fit with the SmartNet CSs, UCs, and market design.

The pilot specification is focused on network monitoring and operation issues more than on the aspects related to market interaction.

The **laboratory test infrastructure** provides higher flexibility than the technological pilots, since it permits, through simulation and emulation, the study of systems and strategies that are currently not deployed. The SmartNet test setup permits to implement and assess diverse network and market configurations, fitting to all CSs and UCs in the project.

In **section 6**, captured ICT requirements are prioritized for each of the sources they are obtained from. Four tables present the main ICT requirements coming from:

- General smart grids framework.
- SmartNet market design.
- SmartNet use cases: business and function level. Latency, information and security requirements are provided.
- SmartNet use cases: information, communication and component level. Network, security, latency, data size, cost and information protocol requirements are provided.

The last **section 7** is devoted to present the conclusions extracted from the document. The main needs and criticalities are presented and reference is made to the ICT requirements summarized in the previous chapter.

1 Introduction

The aim of the present deliverable is to collect the communication requirements for implementing the Transmission System Operator (TSO) - Distribution System Operator (DSO) interaction schemes for the provision of Ancillary Services (AS), as studied in the SmartNet project.

The work is divided into following work actions:

- **Collect security and communication requirements** from TSO-DSO interactions and ancillary service provision.
- **Map requirements ICT functionalities** in business and function layers.
- **Prioritize the discovered requirements** with respect to their importance and realization possibilities.

Five different Coordination Schemes (CS), together with three Use Cases (UC), have been defined in the frame of the project [1]. The first describe various market models, while the use cases define how frequency and voltage regulation services are provided in an AS market framework, which is also being designed in SmartNet [2]. The whole approach involves several communication requirements that are analysed in the present document.

This deliverable D3.1 focuses on business case and functional aspects of the UCs, i.e., the business and function layers as defined by the Smart Grid Architecture Model (SGAM) [3][1]:

- **Business aspects** involve here mainly the market model, i.e. roles/actors and their relationships.
- **Functional issues** refer to the detail of the services, i.e. the steps required to carry them out and, from the ICT perspective, the involved interactions between actors.

The report is divided into seven main **chapters**, that represent the body of the document, plus four more chapters in the annexes. Chapter 2 concentrates on SmartNet coordination schemes, use cases and market design providing the link to the general project framework. Chapter 3 describes smart grid related ICT requirements presented in literature. Chapter 4 presents the SmartNet bottom-up approach, where the requirements are captured from use cases and market features. Chapter 5 describes ICT aspects of SmartNet pilots and puts them in the context of the CSs and UCs. Chapter 6 deals with procedures taken to prioritize the requirements for their further implementation in future tasks of the project:

- Chapter 2: SmartNet Use Case descriptions
- Chapter 3: SmartGrid requirements
- Chapter 4: ICT requirements for SmartNet approach
- Chapter 5: SmartNet pilot and simulation requirements

- Chapter 6: ICT requirement prioritization

The **annexes** in the document present the state of the art of ICT requirements for smart grids. They show the current approach at EU level looking at interoperable solutions for network operation: communication (section 9), information (section 10), security (section 11) and components (section 12). While the project sets the focus on the AS market (enterprise/market zones in SGAM), these chapters provide a broader perspective that can be used as reference of ICT solutions for other project tasks.

The results presented here are a main input for the subsequent D3.2, which deepens into the information, communication and component details of UCs in order to build an ICT architecture.

2 SmartNet Use Case description

2.1 Coordination schemes and use cases

In the frame of the project, five different TSO-DSO interaction schemes have been defined [1]. Their implications on the ICT architecture have been summarised in this subsection.

The main framework of Distribution System Operator (DSO) and Transmission System Operator (TSO) relationship for Ancillary Service (AS) provision is defined by the so called **Coordination Schemes (CS)**. The following are considered in the project:

A. **Centralised AS market model**: the TSO buys the resources from Distributed Energy Resources (DERs) connected to distribution and transmission systems at a centralised market run by the TSO itself. A Commercial Market Player (CMP) aggregates small capacity DER owners and represents them in the market. Two **variants** are considered for this scheme:
    1. Each network operator manages its own data.
    2. The TSO monitors the DSO network.

B. **Local AS market model**: the centralised market is run in the same way as in CS A, but the DSO runs a local market to aggregate distribution network resources. The DSO is a player at the centralised market, where it sells the flexibility resources not used locally. DERs connected at distribution network sell their resources at the local market and those of small size are aggregated by a CMP. Two **variants** are considered for this scheme:
    1. Each DSO organizes a local market, for its individual area, resulting in a one-to-one relationship between each DSO and the TSO.
    2. Several (smaller) DSOs delegate the organisation of one aggregated local market to one Independent Market Operator (IMO), who represents all DSOs in the centralised AS market. This alternative is not considered in the UC descriptions dealing with CS B.

C. **Shared balancing responsibility model**: the TSO runs a centralised AS market, as previously described, and the DSO runs a local market, as in scheme B. However, in CS C, the latter cannot participate in the centralised market, but the TSO establishes set points that the DSO must meet using own distribution network resources. In this case, the following two variants are considered for scheme C. Both start with the outcome of the latest session of the energy market (day-ahead, intraday):
    1. The scheduled profile is determined at an aggregated level for the entire DSO-area (aggregation of multiple points of connection).
    2. The scheduled profile is determined at the level of the interconnection points between DSO and TSO networks.

D. **Common TSO-DSO AS market model**: TSO and DSO contract DER in a common market for different purposes: TSO for AS services and DSO for local system services. The resources are allocated to the TSO and DSO based on a minimisation of total costs. Network constraints are respected. Two variants are considered to this model:
    1. The common market is managed jointly by the TSO and the DSO (extended version of CS A).
    2. In addition to the central AS market, which is managed by the TSO, a local market also exists. The local market is managed by the DSO, who clears the market. However, the final decision on the distribution dispatching programme is taken together with the TSO, to minimize the total costs of both TSO and DSO.

E. **Integrated flexibility Market Model**: there is a common market for AS and DSO services, where all parties participate. It is run by an IMO. TSO and DSO compete for the same distribution network resources.

In addition to coordination schemes and their variants, three **scenarios** (Sc.) are considered to illustrate different levels of DSOs control on the use of distribution network flexibility resources:

- **Scenario 1**: The DSO is involved in the technical and economic prequalification of DER systems to make them eligible for flexibility services provision, while respecting distribution network constraints.
- **Scenario 2**: apart from prequalifying, the DSO can block the activation of resources.
- **Scenario 3**: apart from prequalifying, the DSO sets constraints to be considered in the market clearing process.

The first two scenarios are only applicable to schemes A, D and E, since the local market in schemes B and C already involves the scenario 3 approach. Scenario 2 is not applicable to CS D since the DSO is directly involved in the AS market.

Finally, four **use cases (UC)** are selected for assessment. These are directly linked with services, in particular with frequency control (UC 1 and 2) and voltage control (UC 3) ancillary services. They are defined in the following way:

- **UC 1, Frequency Containment Reserves (FCR)**: related to primary frequency control. It is procured through bilateral agreement or tender (year/month/week/day ahead). Only capacity is offered. One service buyer: TSO.
- **UC 2.1, Automatic Frequency Restoration Reserves (FRRa)**: related to secondary frequency control. It is procured through bilateral agreement or tender. Only capacity is offered. One service buyer: TSO. Activation based on merit order list.
- **UC 2.2, SmartNet Frequency Restoration Reserves (FRR or FRRs)**: extended tertiary frequency control: not only applicable at transmission but also at distribution level; it is

cleared every 5 minutes; and it provides both balancing and congestion management services. Both capacity and energy are procured. Capacity could be year/month/week/day ahead. Procurement and activation happen via fully competitive market place (more than one buyer possible). Available at local markets.

- **UC 3, Voltage Control/Reactive Power for transmission**: central market. The TSO procures voltage control and reactive power provision services via tender. This process is detached from the active power market.

2.2 Actors

Actors are essential part of ICT architecture, because they exchange data in order to fulfil services. Some general definitions in this context are presented below:

- **Actor**: anything that can communicate. Different types of actors can be considered when defining use cases:
  - **Business actor**: an organisation.
  - **System actor**: a function or device. It is connected to a business actor.
- **Party**: organization allowed to participate in markets.
- **Role**: intended behaviour of a business actor.

The next table presents the roles and market parties proposed in the previous tasks of the project [1].

Role	Party
Buyer of DER	Commercial Market Player (CMP)
Market operator	
Seller of DER	DER owner
Aggregator of DER	DSO
Balance responsible	Independent Market Operator (IMO)
Dispatcher of DER resources	TSO
Data manager	
Metered data responsible	
System operator	
Flexibility feasibility checker	

Table 2.1 Roles, parties and system actors

2.3 SmartNet market

This subchapter summarizes the AS market design aspects developed in the project [2] that may have an impact on ICT requirements.

The integrated reserve market is a market for ancillary services aiming to leverage the flexibility from assets located both at the distribution and the transmission grid levels. It is applicable to all the coordination schemes considered within the project.

Regarding **bidding**, these are the main aspects to be considered:

- Within a given market session, a commercial market player (CMP) bids a **price-quantity curve**. Quantity is expressed in terms of energy: positive, for active power injection increase or consumption decrease (upwards flexibility); and negative, for the opposite (downwards flexibility). Prices can also be positive or negative (the bidder wants to receive or pay money respectively). Reactive power is not traded in the SmartNet market but its impact in network operation must be considered and, therefore, flexibility bids must include information on the power factor or a relation between active and reactive power.
- The bid must be associated to a given node of a network. **Locational information** of flexibility assets in transmission and distribution must also be included in the bid,
- **Additional optional information** that might be included in the bid if needed to reflect intertemporal constraints, e.g.: ramping, maximal number of activations over a time horizon, maximal duration of an activation in terms of number of time steps, minimal duration of an activation in terms of number of time steps, minimal duration between two activations, interval of deferability of consumption (for flexible loads), possible complex generation bids...

Timing is defined in accordance to the next concepts:

- Time step: time granularity for market clearing.
- Time horizon: time period considered for market clearing. It is typically a multiple of the time step.
- Frequency clearing: if defines how often the market is cleared. It can be equal to the time step, to the time horizon or in between.
- Rolling optimization: When the frequency clearing is shorter than the time horizon, a certain time step is cleared in different consecutive optimizations (receding time horizon). It allows using the latest information and forecasts.

The **clearing** of the market is done taking into account network constraints both at distribution and transmission levels. The market objective is to optimize the choice of bids activation in order to:

- Solve the imbalance problem at the global level.

- Solve the possible congestion problems in network lines.
- Avoid any voltage problem.
- Maximize social welfare or minimize activation cost.

The market **pricing** is based on the "pay as clear" or "locational marginal price" approach, where the activated bids receive the same price per MWh corresponding to the most expensive activated bid. In addition, a nodal strategy is proposed, meaning that the price is linked to a node in the network.

In addition to the general characteristics mentioned above, some **initial assumptions** are taken in the market design:

- The integrated reserve is a discrete/closed-gate market, cleared frequently (e.g., 5 minutes) and using a rolling optimization (e.g. 1 hour) to take advantage of forecasts (e.g. 12 steps would be cleared at a time, under the previous assumptions).
- When a bidder sends any bid to the SmartNet market, it implies an a-priori commitment from the bidder to the market.
- A bid can be associated to a specific physical asset or to an aggregated portfolio of DER.
- A bid is associated to a specific node of the distribution or transmission grid. The same bid cannot cover assets coming from different nodes of the network.
- A market participant can submit bids for different nodes.
- A market participant can submit multiple bids for the same node but these bids are considered independent.
- The bids are expressed in terms of active power injection/offtake but, associated with it, a power factor will also be provided by the flexibility providers. This allows the market operator to model the impact on the reactive power side of the different activation decisions.
- Quantity is expressed in MW and price in EUR/MW.
- The activation decisions generated by the market clearing are firm for the first step within rolling time horizon. For the rest of the steps within that period, the activation results are not a commitment from the market operator but information about the most likely future activation decisions.

3 Smart grid requirements

Mandate 490 (M/490) given from the European Commission to the European Standardization Organizations in 2011 is central in the context of European Smart Grid standardization and research. The objective of the mandate is to develop and update a set of consistent ICT standards, architectures, processes and services, to achieve interoperability and support the deployment of Smart Grid services and functionalities in Europe. The **Smart Grid Coordination Group** (SG-CG) coordinates the work of CEN, CENELEC and ETSI related to M/490 and has published several reports in response to M/490[3]: reference architecture, proposal of standards to support smart grids deployment, information security aspects, etc. In 2015, the SG-CG was renamed into the Smart Energy Grid Coordination Group (SEG-CG), but the former, more recognizable, acronym is used in this document.

This work performed at European level represents a high level framework of requirements for ICT activities developed within **SmartNet project**: the reference architecture "Smart Grid Architecture Model" (SGAM) [3][4] permits the use case analysis and design using an agreed methodology and is a reference for all ICT related tasks; the communication and information standards proposed by the SG-CG should be respected to meet the interoperability objectives set for the smart grids throughout Europe; and the security aspects should be also taken into account in order to face reliability and data privacy challenges linked to ICTs.

Based on these developments, a summary of communication, information and security aspects is presented in the annexes, as reference for ICT architecture development within SmartNet. They help understand the available technological choices for information exchange in the context of network services development. The smart grid requirements suiting best the SmartNet approach, which is focused on the AS market, are presented in the subsections below.

3.1 Communication technologies

The types of networks more directly linked to AS market processes are the following (we keep the letter referenced as in [5], see section 9 for additional information):

G. **Intra-control centre / intra-data centre network**: they provide connectivity for systems inside the same facility and connections to external networks. Both networks are at the same logical tier level but control centres connect to real time systems with high levels of security. It is suited for the transmission of messages between different applications located in servers within the same company or group of companies, e.g. LAN network connecting DSO DMS and DSO trading systems.

H. **Backbone network**: inter-enterprise network, including backbone internet, as well as inter-control centre networks. It is suited for the connection between different actors, e.g. for the

connection of market participants with the market platform or for the connection between DSO and TSO.

The communication technologies most commonly used (in bold) and/or suitable for each network type [5] are mapped to the SGAM framework in the figure below. The area in blue indicates the domains and zones of the smart grid covered by both network types. They link systems devoted to the centralised operation of networks, with the applications dealing with commercial and organizational processes and with market trading systems, within the same company or among different companies, and in all network domains, from transmission to customer premises. Several options exist for each zone and domain, and the final architecture deployed should be assessed case per case based on the service to be provided, availability, cost, etc.

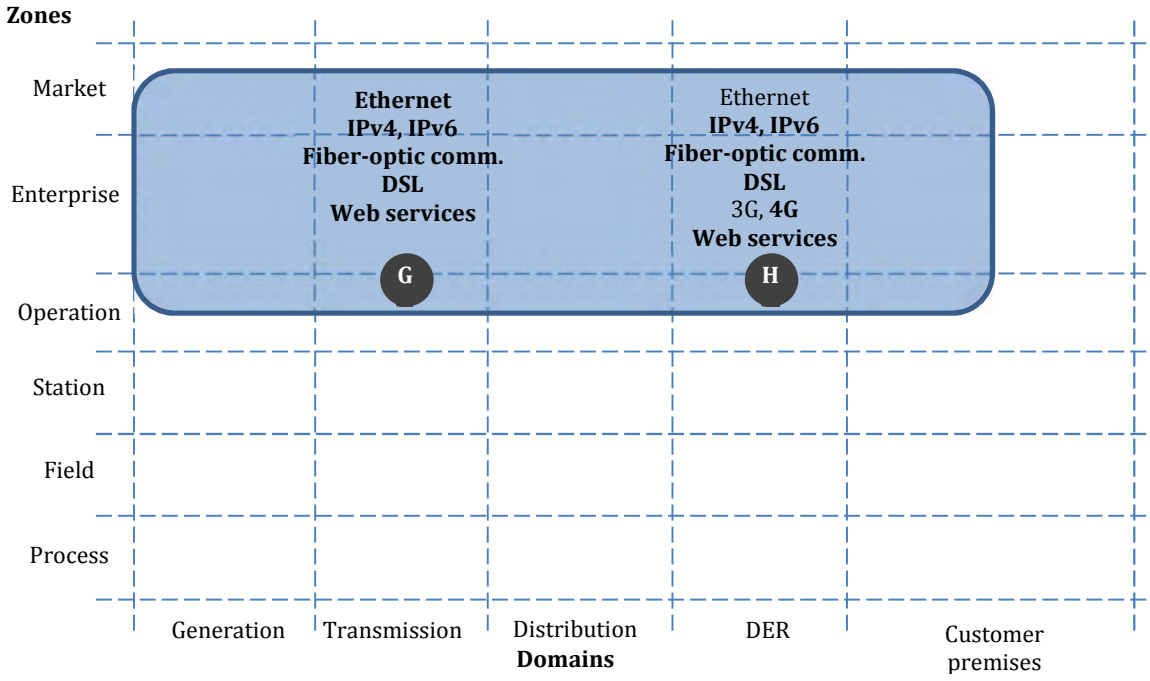


Figure 3.1 Overview of smart grid communication technologies mapped to SGAM

The technologies in the figure above are those proposed by the SG-CG. However, there are other technologies currently under development, such as 5G or Narrow Band Internet of Things (NB-IoT), that will become widely deployed in the future and need to be acknowledged as new opportunities for Smart Grid communications.

SmartNet focus is on ancillary services market and the design of this market (see section 0) sets clear requirements on time limits and amount of information to be exchanged within every discrete market step. In principle, market related operations are not "too" time demanding, since they do not require real time operation. Therefore, most common current technologies could be eligible from **latency** point of view (this needs to be assessed during the ICT architecture design).

A classification contained in the IEC 61850-5 standard [6] is taken as reference for latency requirements of smart grid functionalities. The next Table 3.1 shows the transfer time (latency) considering, apart from the communication itself, both coding and decoding of information processes, and it is independent of the number of control levels (e.g. intermediate nodes between end-to-end points).

Perf. Class	Requirement description	Transfer time		Application
		Class	ms (≤)	
P1	Total transmission time below the order of a quarter of a cycle (5ms)	TT6	3	Trips, blocks, releases inside substation or other local system
P2	Total transmission time in the order of half a cycle	TT5	10	Trip, block, release messages between substations or local systems
P3	Total transmission time in the order of one cycle[1]	TT4	20	Fast automatic interactions less demanding than the "trip"
P4	Transfer time for automation functions is less demanding than protection type messages but more demanding than operator actions	TT3	100	Slow automatic interactions (normal state information, less time critical automation messages...)
P5	Total transmission time half of the operator response time (≥ 1s) regarding bidirectional events	TT2	500	Operator's commands: reading / changing set points, presentation of system data, auto-control functions
P6	Total transmission time in line with the operator response time of ≥ 1s regarding unidirectional events	TT1	1000	Normal event and alarm handling, temperature measure...
P7 (P1)	Delay acceptable for protection functions using these samples	TT6	3	Samples (e.g. for protection functions). Outputs from digitalizing transducers and digital instrument transformers (IED data)
P8 (P2)	Delay acceptable for other functions using these samples	TT5	10	
P9	**Not critical transfer time. Files with process data for post-mortem analysis or off-line statistics. Bit length (PICOM) ≥ 512 bits**	**TT0**	**10 000**	**File transfer functions: disturbance recording, information, settings for IEDs**
P10 (P5)	Total transmission time half the operator response time (≥ 1s) regarding bidirectional events	TT2	500	P5 message with access control
P11 (P6)	Total transmission time in line with the operator response time of ≥ 1s regarding unidirectional events	TT1	1000	P6 message with access control
P12 (P9)	Not critical transfer time. Files with process data used for post-mortem analysis or off-line statistics.	TT0	10 000	P9 message with access control

Table 3.1 IEC 61850-5 performance classes and requirements

According to this table, market processes considered in SmartNet would be assigned to the transfer time class TT0 (transfer times lower than 10 seconds). Nevertheless, as smart grids deployment grows,

[1] The performance for automation functions are typically between the response time of operators (order of 1 s) and of protection (order of 10ms).

lower latencies are likely to be needed. Moreover, safety margins and shorter market steps require also a faster message exchange.

When designing an ICT system for smart grids, the features provided by the chosen communication technologies should respond to these requirements. Elneel presents the following mapping between communication technologies and transfer time requirements in Table 3.2 [7].

Type/application	Latency requirements	Network technology
Type 1A - Trip (fault isolation & protection)	3-10ms (P1/P2)	Fiber optic communication, Metro-Ethernet, High performance microwave
Type 1B - Other IED automation	20 ms (P3)	Fiber optic, Metro-Ethernet, High performance microwave, LTE-advanced
Type 2 - Medium speed control	100ms (P4)	LTE, WiMAX and above
Type 3 - Low speed control	500 - 1000 ms (P5/P6)	PLC, RF-mesh, 3G, LTE, WiMAX and above
Type 4 - Continuous Raw IED data messages	3-10ms (P7/P8)	Fiber optic, Metro-Ethernet, High performance microwave, future LTE-advanced
Type 5 - File transfer functions	≥ 1000ms (P9)	PLC, RF-mesh, 3G, LTE, WiMAX and above

Table 3.2 Network technologies for network latency requirements [7]

Complementing the information in the previous table, the forthcoming 5G technology is anticipated to extend the use of wireless communication towards fast automatic interactions.

An example of ICT data rate requirement calculation to meet some smart grid applications is provided by Kuzlu in [8].This reference was taken as basis to build the next table.

Application	Data source (units)	Message size (bytes)	Latency (seconds)	Data rate (kbps)
On-demand meter reading	625 meters	100	5	100
Multi-interval meter reading	625 meters	1600-2400*	10**	800-1200
Load management	500 customers	64	5	51
Distribution automation	15 IEDs***	150-500	1	18-60
Synchrophasor	100 PMUs	48	0,0167	2300

* 100 bytes x 4 messages per hour x 4-6 hours/reading interval
** From Table 3.1. Higher latencies could also be valid
*** 15 field devices per 1000 meters is a typical value according to [8]

Table 3.3 Data rate calculation example for some smart grid applications

Other properties to be considered for communication technology selection are the following:

- Bandwidth (related to data rate).
- Coverage.
- Architecture scalability.
- Ownership (private or public network).
- Access layer density.
- Interface flexibility.

- Operating and capital expenditures.
- Reliability and security.
- Open standards support.

3.2 Information standards

There are already information exchange standards available that are designed for energy market environments. Some of those data models can be exploited and used in the development of energy services in the market context.

The information that needs to be exchanged between business actors and their systems is also a vital input for ICT architecture design. The amount of information to be sent and received, as well as its criticality, sets requirements for communication, computational and data base capabilities of smart devices and backend systems. When deriving ICT requirements, the following information exchange **features** needs to be considered:

- Data model (exchanged types of data).
- Average data size.
- Implementation complexity.
- Availability in market solutions.
- Open or restricted (international/de facto/proprietary standard).
- Security.
- Legacy of old versions and technologies.
- Required communication technologies.

Some of the most important standards and protocols in the smart grid environment, according to the CEN-CENELEC-ETSI Smart Grid Coordination Group SG-CG [3][5], have been analysed, in order to understand the already defined data models that might be used for information exchanges leading to network services provision. This knowledge allows us to match requirements to existing developments or/and to identify gaps according to the needs of the project. A short description of the standards is provided later in section 10 of this report.

The standards that suit best market exchanges are the following:

- **EDI**: which is not really a standard but a library by ENTSO-E containing several documents and definitions for the harmonisation and implementation of standardised electronic data interchanges in the context of achieving EU energy policy goals. The Market Data Exchange Standard (MADES) is comprised of standard protocols and utilizes IT best practices to create a mechanism for exchanging data (documents) over any TCP/IP communication network, in

order to facilitate business to business information exchanges as described in IEC 62325-351 and IEC 62325-451 standards.

- **IEC 62325:** it is a set of standards describing a framework for energy market communications. Its main parts are covering the communication between market participants and market operators. The common information model (CIM) specifies the basis for the semantics for this message exchange [9].

The following table shows the main data types supported by these two standards.

Type of data to be exchanged	EDI	IEC 62325
Market context definition	■	■
Market document / messages exchange (secure)	■	■
Market business process implementation methodology	■	
Capacity allocation and nomination: congestion management and scheduling	■	■
Acknowledgement of business process in markets		■
Scheduling information	■	■
Reserves resources information: tendering planning and activation.	■	■
Settlement data (imbalance reports, metered information, finalized schedules...)	■	■
Problem settlement and status request in market processes		■
HVDC scheduling	■	
Information for interconnection capacity determination from critical network elements	■	

Table 3.4 Market data types in ICT standards and protocols

The fields above mapped to the Smart Grid Architecture Methodology (SGAM) affect Market and Enterprise zones for all domains.

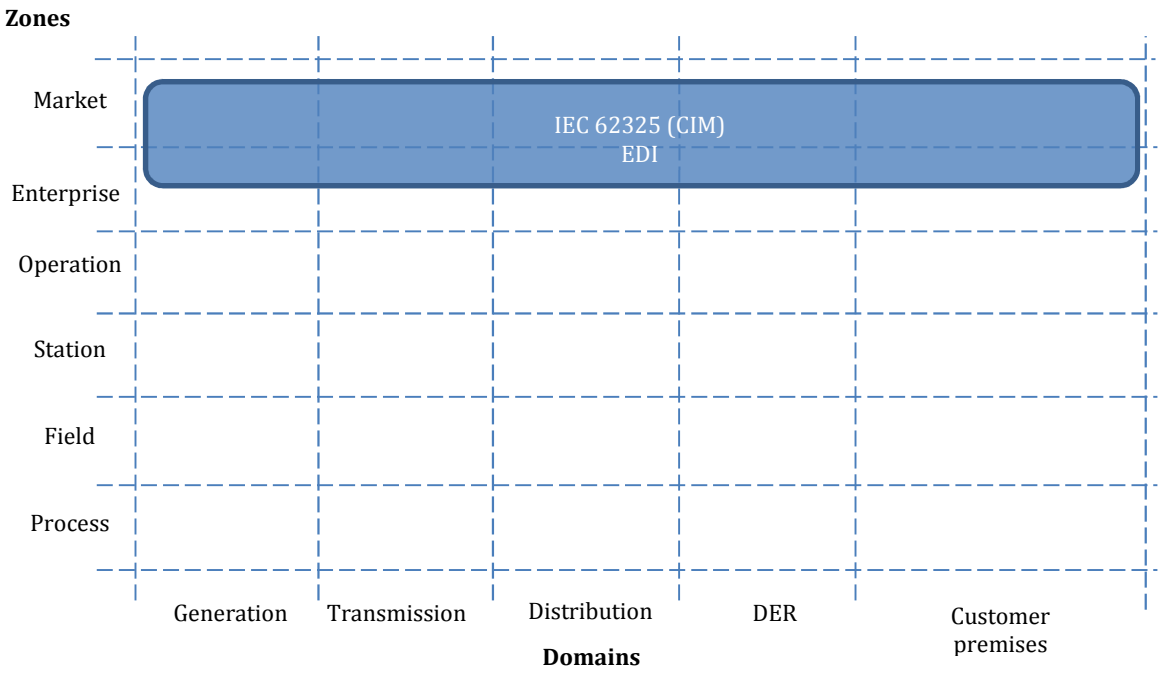


Figure 3.2 Mapping of market data types to the SGAM zones and domains

3.3 Security aspects

In theory, communication problems leading to the inability to exchange AS market related information could cause **reliability** problems at country or, even, at European domain, depending on the importance on a national market on the surrounding systems. This means that security levels 3/4 (high/critical) defined by the SG-CG (see Table 11.1) needs to be considered when communication requirements for TSO-DSO interaction are designed.

Currently, energy markets already rely on ICTs to perform various kinds of information exchanges. The probability to have a communication blackout causing the inability to perform the market clearing is very low. In addition, as mentioned before, latency is not a critical issue compared to that of other smart grid functionalities and small delays on the transfer time can be tolerated without causing a system emergency.

In relation to **data integrity**, encoding and the use of digital certificates are currently widely deployed in information exchanges with market platforms. However, this does not diminish the relevancy of integrity, availability, confidentiality, authentication and non-repudiation (see section 11) when capturing requirements for communications.

There are already recommendations for ICT systems to improve their reliability and security [10]:

- **Hardware redundancy**: critical parts of the system are duplicated, e.g. data centre, control centre, communication mean, etc.

- **Data redundancy**: data is duplicated in more than one place within a computer system, e.g. by running two hard disks in parallel, disk mirroring.
- **Software redundancy**: more than one routine, written by independent coding teams, is produced. If there is no software failure all models produce the same output given the same input. If there is a disagreement a voting logic determines the operation. However, this could be seen as overkill for all but the most safety-critical systems: formal verification and full test coverage would perhaps be a more practical and cost-efficient approach.
- **Time redundancy**: performing the same operation multiple times, e.g. multiple copies of data transmitted.
- **Backing up**: the data is stored (duplicated) in separate locations, e.g. buildings, distributed clouds, etc.
- **Alternative paths for data transmission**: apart from hardware redundancy, meshed topologies permitting the dynamical selection of the best paths present better reliability levels.

The reference standard for security in smart grid environments (e.g. IEC 61850) is the IEC 62351, while the IEC 27019 TR is a reference for process control systems and automation technology in the industrial sector, including utilities.

4 ICT requirements for SmartNet approach

ICT requirements have been collected both in top-down and bottom-up manners. The use case descriptions introduced in section 2 have been studied from the ICT's point of view. Two iteration cycles were performed, during which feedback was given to the task in charge of defining the UCs, and the ICT requirements were refined. During the study phase, ICT system illustrations were created to highlight the interactions between actors. For each connection, the information exchange was evaluated and ICT requirements were defined. Definition of ICT requirements for all use cases is a daunting task and, therefore, they have been classified into the categories that are presented in the previous chapters:

1. Network requirements
2. Security requirements
3. Latency requirements
4. Data protocol requirements
5. Technology related requirements

The Enterprise Architect (EA) tool with the SGAM toolbox extension has been used to model ICT functionalities and derived requirements at business, function, information, communication, and component layers. The use of a common format enables to share the information through different developers and final-users in an effective way.

The ICT requirements described in this report are the foundation for the design of the SmartNet ICT architecture, which will be presented in SmartNet deliverable D3.2. The ICT requirement specification and architecture design work utilises the following sources:

- High level framework set up by the general smart grid approach at European level.
- The coordination schemes represent the business layer in the SGAM, i.e. the involved actors/roles and their relationship (market model).
- The use cases represent the function layer in SGAM, i.e. they detail the characteristics of the services to be exchanged in the SmartNet market.
- The SmartNet market characteristics set requirements from the business to information layers in specific aspects related to market operation.

4.1 Coordination schemes

The coordination scheme descriptions define the market models linked to business cases, while related variants and scenarios introduce additional requirements for the communication architecture.

To describe the business cases, business actor roles are used in the present analysis. The use of roles helps keep the schemes valid for different system implementations, in which stakeholders may play different roles in accordance to the local legislation. The following business actors are considered for SmartNet coordination schemes:

- **System operator**: TSO. The TSO is also normally the buyer of AS in the central market.
- **Grid operator**: DSO. The DSO is, under some coordination schemes, the buyer of AS in the local market. System and grid operator denominations are taken from the ENTSO-E role model [30] to differentiate between actors in the transmission and distribution networks.
- **Market operator**: according to the defined coordination schemes this role can be played by the TSO, DSO, TSO and DSO together, and IMO.
- **Aggregator**: it aggregates the service offer of DER owners that are not allowed to participate in the market or that prefer to do it in an aggregated way. It is also a seller of flexibility in central or local markets and, therefore, a CMP. For simplicity, in the business case schemes it is considered that it only aggregates DER owners in distribution level.
- **Seller**: DER owner not requiring aggregation, it is also a CMP. For simplicity, in the following schemes it is considered that only DER owners in transmission participate directly in the market Even if this simplification is far from real because the number of CMPs in distribution is increasing in some systems (e.g. in Denmark), it does not prevent the analysis of DER - market connection type, which is the scope here.
- **Flexibility provider**: this term, not introduced in previous project tasks, represents the role of DER owners not participating directly in the market but through an aggregator. For simplicity, it is considered that all DERs connected to distribution participate in markets through an aggregator, and that DER owners in transmission do it always directly, although also they would play the role of flexibility providers apart from that of sellers.

The business cases defined in this study for the different coordination schemes are summarized in the following subsections. The provided schemes, depicted in EA, have the following common features that should be considered for a correct interpretation of the figures:

- **Business actor**: as defined above.
- **Business goal** (green box in the diagrams): main business goal of the business actor (related to the AS exchange).
- **Business use case** (yellow ellipse): use case developed by the business actor and devoted to achieve the defined business goal.

- **High level use case** (blue ellipse): functional use case (service), which is equivalent to SmartNet use cases. It defines the functionalities permitting to develop the business use case. They are further developed at function layer level (see section 4.2). They are linked to the TSO in CS A, B C, and D; and to the IMO in CS E. The high level UCs of other actors are related to the former and described through their steps.
- **Dashed line** (with the label <<flow>>): it indicates that a communication link exists between the involved business actors.
- **Continuous line**: it indicates an association between business actors, e.g. contractual relationship (flexibility contract, for example), market rules, etc.

4.1.1 Coordination scheme A

This is the most common approach in current power systems in Europe. The CS A business case is presented in the next Figure 4.1.

Some of the main characteristics of this CS are the following:

- The TSO participates at the market as buyer of services and also managing it, i.e., the TSO plays both system operator and market operator roles. This means that the communications between the system operator and the market operator are intra-data centre communications as defined in section 3.1.
- DSO is not procuring local flexibilities in real-time or near to real-time. In Figure 4.1, it is mentioned that the DSO can use flexibility in distribution, but this is long term ahead procurement.
- A general assumption, for all coordination schemes, is that all market related communications, from bids to settings and blocking signals, are performed through the market operator platform. Direct communications between DSO and TSO control centres are reserved for emergency situations and, therefore, out of the scope of SmartNet.

4.1.2 Coordination scheme B

The CS B business case is presented in the next Figure 4.2.

Some of the aspects explained for the previous CS A are also applicable here, therefore the focus is set on the new aspects linked to CS B:

- The distribution flexibility aggregator (CMP) offers its resources, not in the central, but in the local AS market.
- After a local optimization takes place, the DSO sells surplus resources at the central market and becomes a CMP under this scheme.

4.1.3 Coordination scheme C

Coordination scheme C considers that local and central AS markets run in parallel, and that the TSO establishes settings to be met by the DSO, either zonal or by node. This last fact does not affect the communication links but it will affect the data models and the size of the messages to be exchanged.

The main differences, compared to the previous case, are the following:

- No participation of DER resources connected at distribution network is expected in the central AS market.
- The TSO defines some operation settings to the DSO and these will be transmitted also through the central market platform.

The scheme is described in Figure 4.3.

4.1.4 Coordination scheme D

Coordination scheme D consists of two variants directly related to some of the previous CSs:

- **Variant D1**: it is an extension of CS A, in which the central market is not run only by the TSO but by both the TSO and DSO together. It is to be established if this joint work would mean a new market actor depending on both DSO and TSO parties. Figure 4.1 would still be valid to represent this scheme. Only the nature of the communication link and the types of messages exchanged between the grid operator and the market operator would be different with respect to CS A.
- **Variant D2**: this scheme represents an extension of CS B. Central and local markets exist but, in this case, before the local market is cleared, the TSO needs to be informed to check possible negative effects in the transmission network and minimize total network costs. This fact does not represent any variation at market model level with respect to the one presented in Figure 4.2.

4.1.5 Coordination scheme E

The main aspect introduced by this scheme is summarized below:

- The common AS market is managed by an IMO and, therefore, both the system and grid operators become an additional CMP. They both sell and buy products at the AS market.

This scheme is presented in the next Figure 4.4.

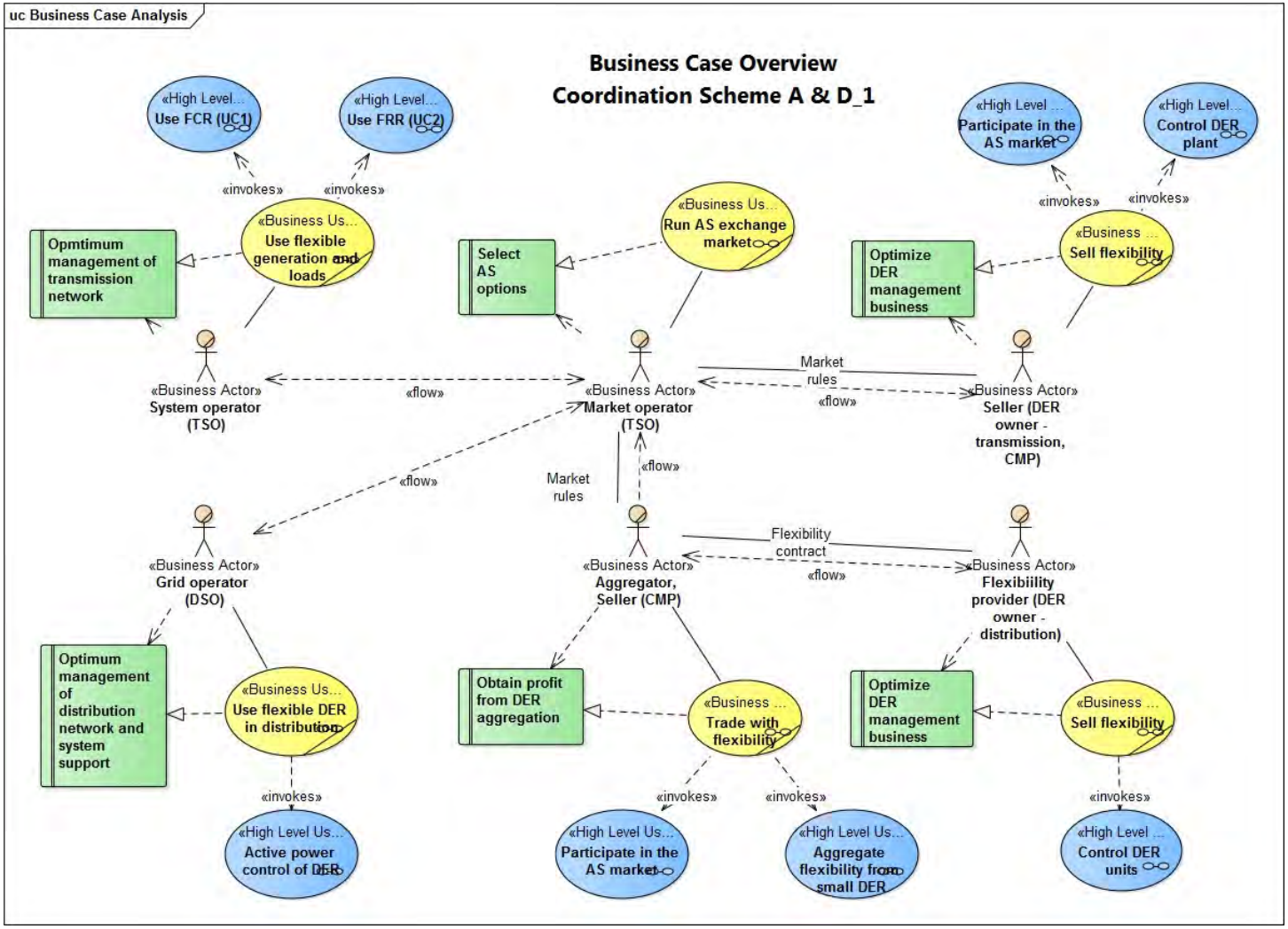


Figure 4.1 Coordination schemes A and D1 market model

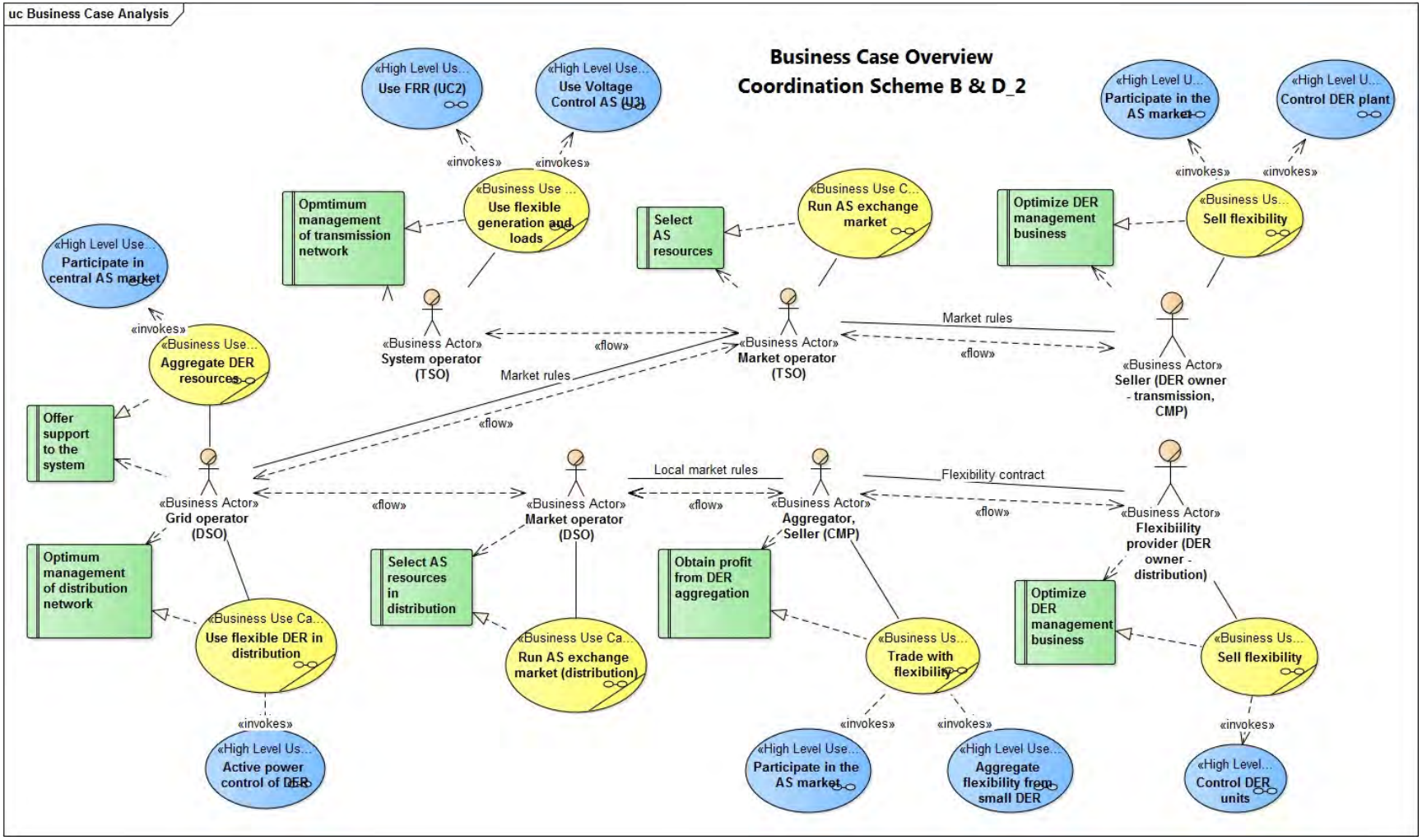


Figure 4.2 Coordination scheme B and D2 market model

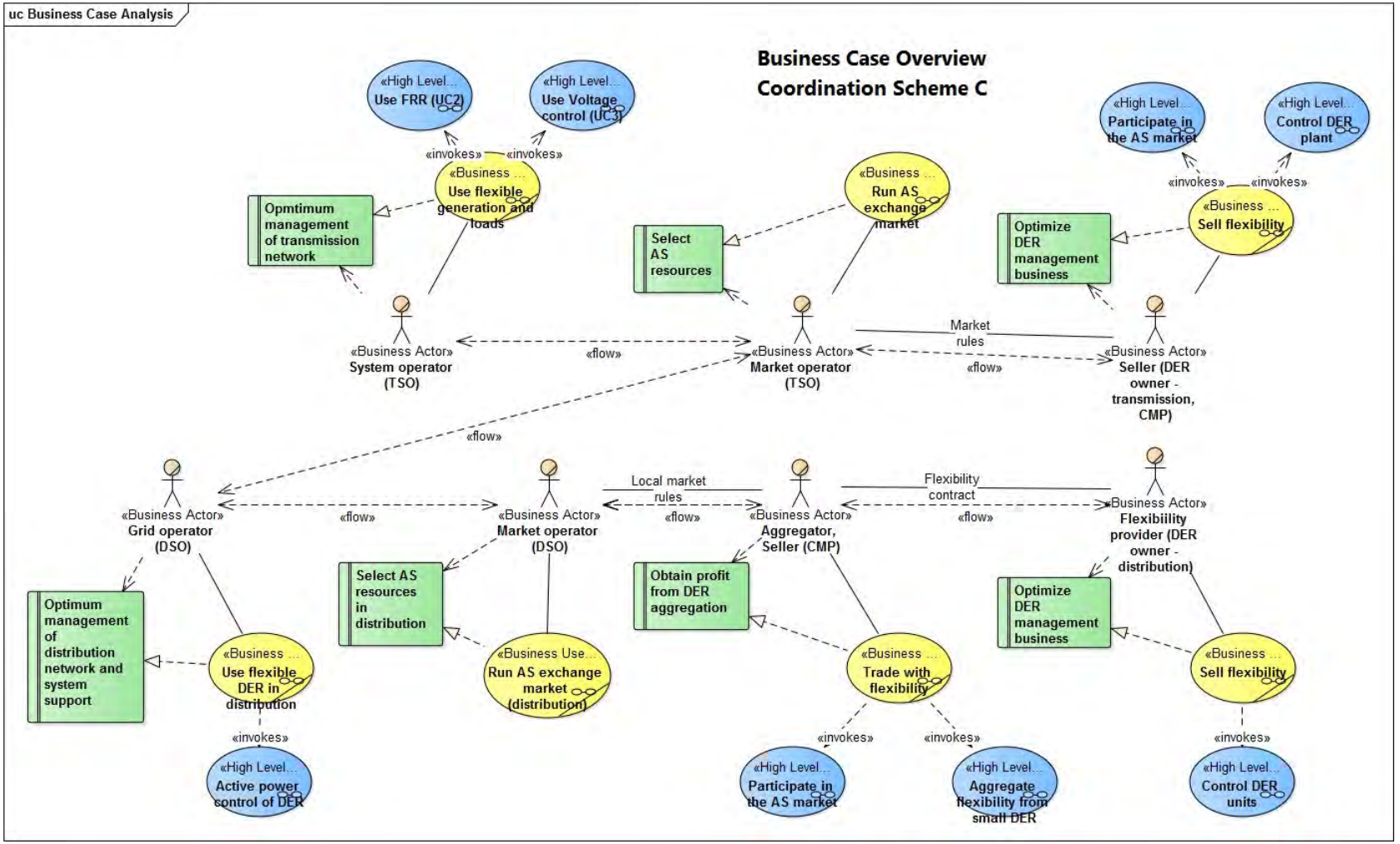


Figure 4.3 Coordination scheme C market model

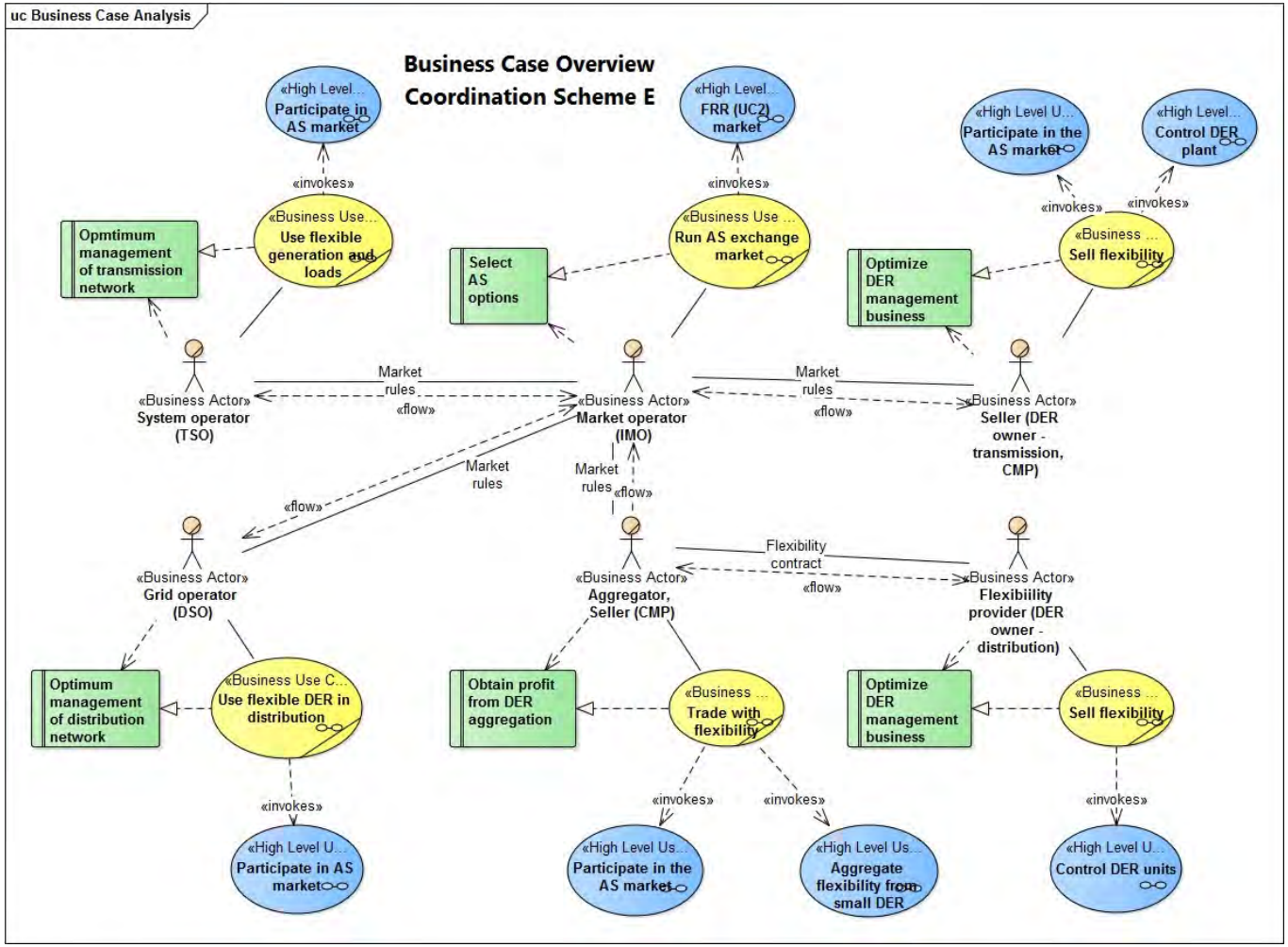


Figure 4.4 Coordination scheme E market model

4.2 Use cases

To capture ICT requirements from the UCs, the ELECTRA template [11] was utilised and tailored to SmartNet necessities. The following use cases have been an input for this study:

- Frequency control (UC1): applicable to CS A and D.
- Balancing and congestion management (UC2): five use cases, one for each CS (from A to E).
- Voltage control (UC3): applicable to CS B, C and D.

The use cases have been divided into four main processes that are common to all of them: **pre-qualification**, **procurement**, **activation** and **settlement**. Pre-qualification and settlement (excluding real time monitoring processes) are the less time critical processes from the ICT point of view, because they are normally detached from the intra-day operation of the network.

To describe the functional relationship within the use cases, a set of **system actors** was assigned to the business actors' roles defined in the previous subsection. System actors are in line with the most common smart grid components defined by the SG-CG (see section 12 for more details). The relationship between business and system actors, linked to business and function layers in the SGAM model respectively, is defined in the following Table 4.1.

Business layer		Function layer	
Market party	**Business actor (role)**	**System actor**	**Description**
TSO	System operator	EMS (Energy Management System)	EMS refers, here in general terms[2], to the applications used by the system operator for network management (operation zone)
		Trading system	Application used to interface with market mgmt. systems (enterprise zone)
TSO	Market operator	Market mgmt. system	System used to run the central energy market and to exchange non-critical information with the system operator[3]

[2] This definition is not strictly limited to the EMS in our case: all applications for system management are included under this definition (e.g. SCADA, the outage management system, etc.).

[3] As mentioned above, the **market platform** is used for all communication between the market operator and the market participants, not only for economic data exchange (procurement, settlement...), but also for operational non-critical data exchange (e.g. schedules and settings), considering "non-critical" everything that is not real time. Real time operation requires other communication architecture, security level and protocols.

Business layer		Function layer	
Market party	**Business actor (role)**	**System actor**	**Description**
DSO	Grid operator[4]	DMS (Distribution mgmt. system)	DMS, here in general terms[5], refers to the applications used by the grid operator for network management (operation zone)
		Trading system	Application used to interface with market mgmt. systems (enterprise zone)
DSO	Market operator	Market mgmt. system	Market management system used to run the local energy market and to exchange non-critical information with the system operator[6] (market zone)
IMO	Market operator	Market mgmt. system	Market management system used to run the energy market and to exchange non-critical information with the system operator (market zone)
CMP/DER owner transmission	Seller	EMS	Applications used by the DER owner for plant control (operation/station zone)
		Trading system	Application used to interface with market mgmt. systems (enterprise zone)
CMP	Aggregator (distribution)	Trading system[7]	Application used to interface with market mgmt. systems and with DER owners (enterprise zone)
DER owner in distribution[8]	Flexibility provider[9]	EMS	Applications used by the DER owner for plant control (operation/station zone)
		Trading system	Application used to interface with the Aggregator (enterprise zone)

Table 4.1 System actors for UC description

The process steps associated with respective use cases have been described at the function layer level in coherence with the SGAM methodology. The seven input use cases have been analysed and integrated into a generic use case, which consists of the aforementioned four processes and describes their most significant ICT requirements. It is expected that some of the messages in data models will be different depending on the service type, but the process steps should remain practically the same. The use case specific requirements are input for the design of the ICT architecture.

[4] It should be **system operator** in accordance to the naming in previous project tasks. Here is used the ENTSO-E role model differentiation between TSO and DSO (system/grid operator).

[5] Similar to note 2.

[6] Similar to note 3. The local market is considered to follow the same principles as the central market.

[7] It is considered that the **aggregator** does not control directly DER plants but transmits settings, prices, etc.

[8] It is not a market participant because it is aggregated by the CMP. Some **DER owners in distribution**, due to their size, may not need aggregation but, from the ICT point of view, this fact does not add much new to the UCs, since these actors can be considered in a similar way to DER owners in transmission, especially when they participate directly at the central market or when local and central markets follow the same design (this is the approach in SmartNet).

[9] This is not a role defined previous tasks of the project.

The four processes of the integrated function layer are described in the next subsections through activity diagrams that illustrate differences in specified CS, variants and scenarios. They show the steps in each process and, from them, general ICT requirements are derived, mainly regarding data models.

4.2.1 Pre-qualification

Pre-qualification is the process through which flexibility provider's eligibility to participate in the AS market is assessed. It can deal both with technical aspects (technical capability of systems) and with market aspects (capability to meet market rules, e.g. minimum size, technology type...). DSO pre-qualification related to distribution system constraints in central market (scenario 1) is not considered here.

Two types of pre-qualification have been considered. The most common one, here called l**ong-term prequalification**, is expected to be detached from the day-ahead and intraday market operations. It could be performed yearly, quarterly, etc. Normally, it is based on the submission of detailed technical features of the flexibility resource or third party certificates, by the CMPs to system operators (always through the market platform according to our approach). The system operators would then evaluate the technical feasibility of these flexibility providers to offer the requested services. In some cases, real tests might be required to assist this evaluation. Also this option is included in the activity graph through an alternative path that may affect both the TSO and the DSO procedures during the pre-qualification.

Those coordination schemes with local market structures (B, C, D2) have additional steps related to local market processes. Because of this, the number of messages and computation periods to be fitted into the market steps is higher for these schemes.

The **short term pre-qualification** (day-ahead) is not common in current market structures. It is proposed to get more precise information about the flexibility capacities of service providers, considering that they may change depending on network and system conditions. This type could be linked to e.g. UC3, where the system operator sends voltage and power factor settings for the next day in accordance to the flexibility capacities of providers without the existence of a reactive power trade market. Under this assumption, the service provider may update its reactive power capacity on day-ahead basis. Updates would be always upgrades above the long term pre-qualified capacities.

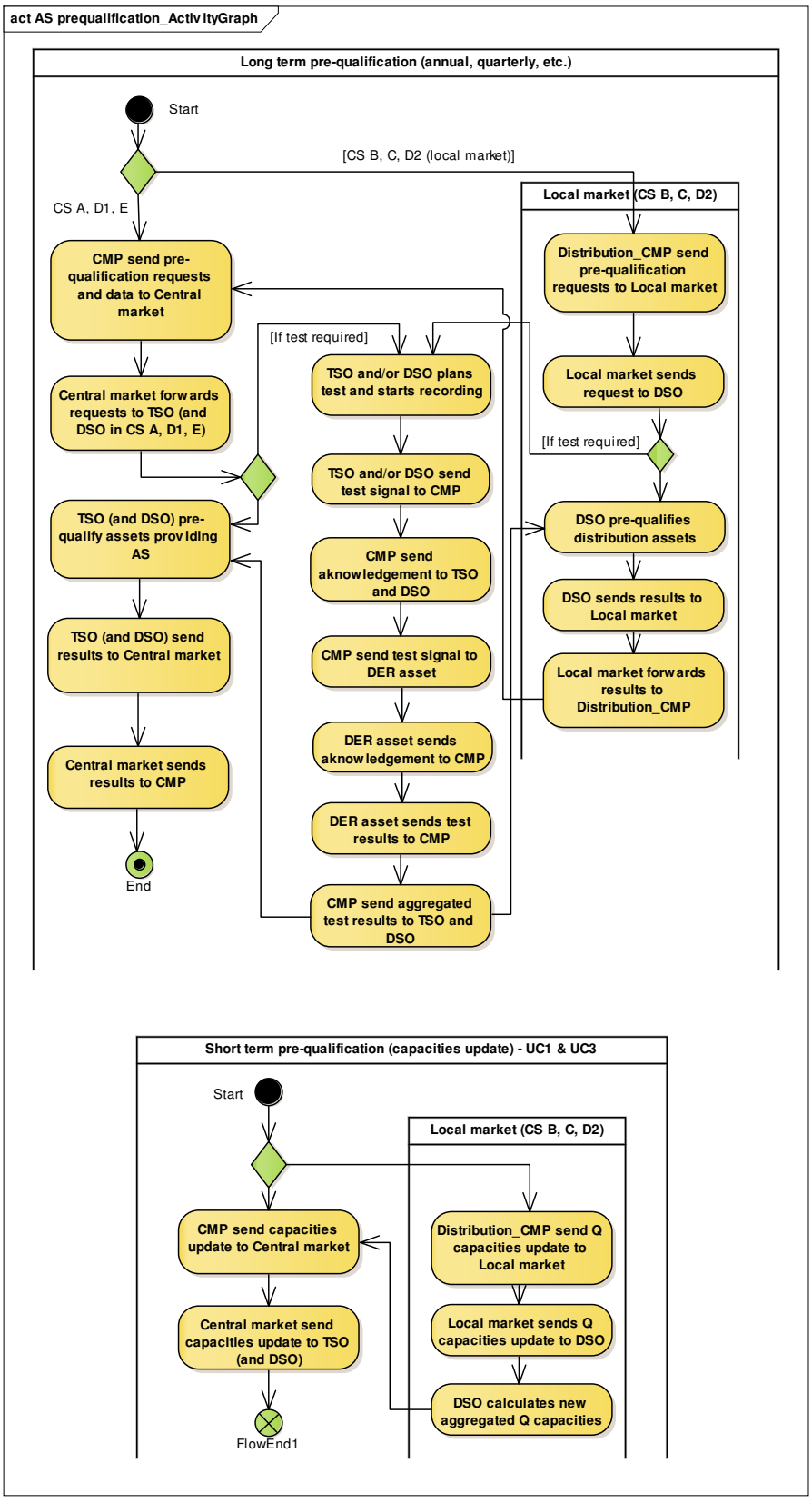


Figure 4.5 Use Case pre-qualification process activity graph

According to this activity diagram the following ICT requirements are identified.

- From the **communication networks'** point of view, some links between system actors need to use backbone networks, while others require intra data-centre networks. This is common to all four processes and different ICT requirements in terms of security, technology options, costs, etc. can be derived from each type of network.
- From the point of view of **data models**, the following message types need to be exchanged between actors:
    - **Pre-qualification request message** (from the CMP): market regulation should make clear what information should be included by flexibility providers in this pre-qualification request messages: technical features, third party certificates if needed, etc. In principle, messages could be similar for both central and local markets and for all UCs 1, 2 and 3.
    - **Pre-qualification result message**: same remarks as before. It should inform DER owner if their systems are eligible to provide AS.
    - **Test signal**: for the activation of pre-qualification tests. This could contain just start and end times for the test or it could be elaborated to have more information regarding test characteristics.
    - **Acknowledgement message**: this is a message that needs to be used in different occasions within UCs to confirm the reception of important messages. It could have a common structure in all cases (e.g. time stamp and an identifier of the corresponding message).
    - **Test result message**: they are based on local measures taken in the DER system providing AS.
    - **Aggregated test result message**: it is the message that an aggregator of DER assets should send to system operators with the aggregated test result of its portfolio of flexible systems. Both the aggregated and the single test result message could have the same format.
    - **Capacities update message**: it contains the new capacities that the flexibility provider can offer to the market. It is linked to reactive power and droop capacities update (upgrade) by flexibility providers.

4.2.2 Procurement

Procurement refers to the market procedure devoted to the selection of the best AS bids, from an economic point of view.

In market contexts, the activation of selected providers through a real time signal is not required because, as a result of market clearance, all providers know when to start and stop their systems. For this reason, the boundary between procurement and activation is not clear. We have taken the following assumption, which does not have real implication on ICT requirements:

- **Procurement**: it starts with the definition of reserve requirements by system operator(s) and it ends with the sending of the market clearance results to the system operator(s). As a result of market clearance, the bids are selected based on economic offers and the marginal pricing method defines the price to be paid for those resources that will be activated.
- **Activation**: it starts with the technical constraint assessment of market clearance results by the system operator, and it ends with the dissemination of schedules and settings to CMPs. The schedule is obtained from the application of technical constraints to the outcome of the market economic clearance. The settings are defined from simulations by the system operator based on the long term and short term pre-qualification information.

SmartNet procurement process is linked to UC 1 and UC 2 where active power is traded. In accordance to SmartNet market design, reactive power is not traded in itself, even if it must be possible to assess its impact from the information contained in the bids. Therefore, UC 3 would have no procurement phase.

Procurement, as presented in next Figure 4.6, has two main paths: those steps for the central AS market (common to all CSs) and those specific for the local market (CS B, C and D2). However, there is a difference in the latter that affects the order of actions. In CS B and D2, results from the local market may affect the participation in the central market (e.g. the DSO could offer at the central AS market the resources not used in distribution). However, in CS C the DSO should get the resources from the local market that would help him to meet the schedule defined by the TSO. As consequence, the local market processes come after those of the central market.

The DSO is considered just another CMP in CS B. This is why no specific mention is made to it in the bid submission step in the graph.

Another, alternative path is depicted in the graph to show scenario 3 under CSs A and E. In CS A, the DSO does not participate in the central market but, still, it has to communicate distribution network constraints. As consequence, a communication link is established with the market operator.

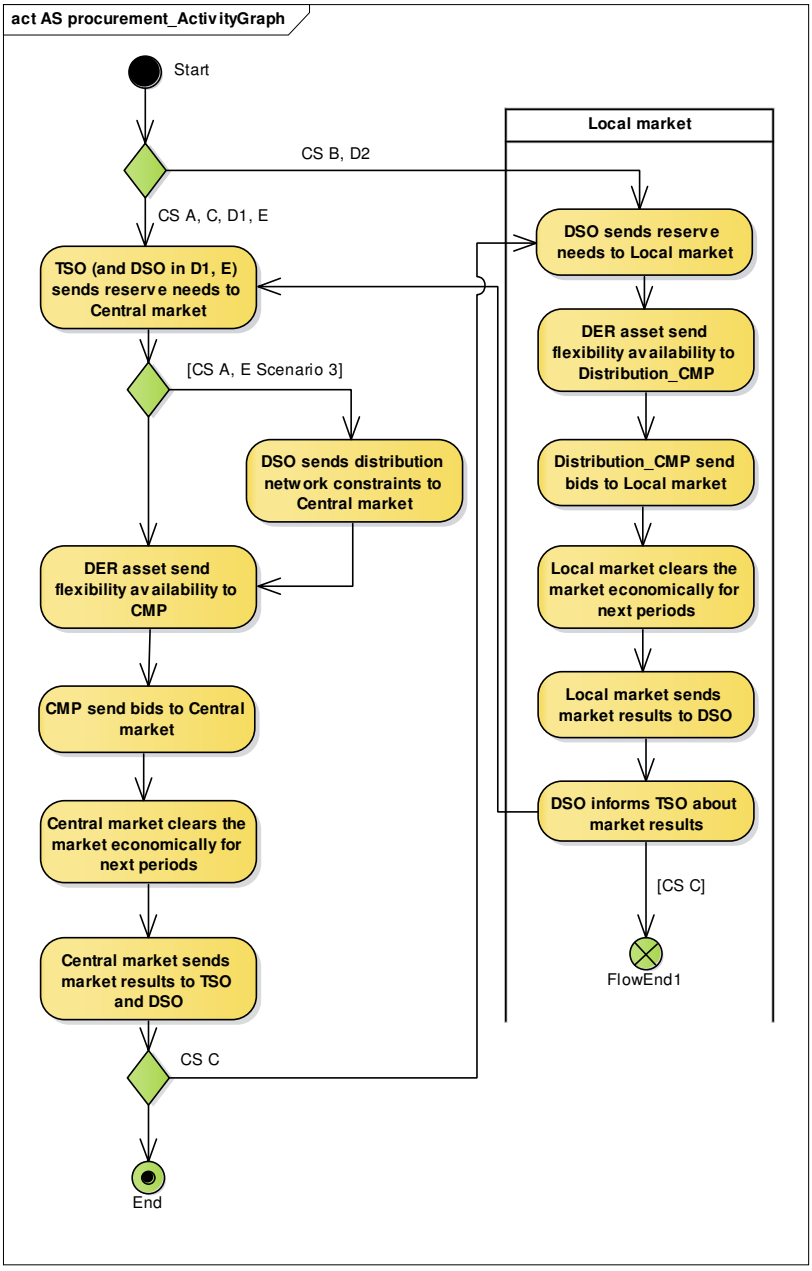


Figure 4.6 Use Case procurement process activity graph

From the point of view of data models, the following message types need to be exchanged between actors:

- **Reserve needs message**: it would be based on an active power versus time curve.
- **Distribution network constraint message**: it should indicate the limits (power, voltage or other) of the areas/nodes in the distribution network to be considered in the central market clearing process.

- **DER flexibility message**: DER resources send to the aggregator their flexibility for the next hours or market sessions.
- **Market bid message:** CMPs **(**DER assets, aggregators and DSOs in CS B) indicate which active power flexibility they have for the next market periods.
- **Market results message**: this message should indicate at least, for each market period under definition, the assets selected to provide the service, the active power provided by that asset (up or down) and the locational marginal price.

The message formats could be common for the central and local markets, even if some of the parameters would not be applicable or meaningful for both (e.g., in this case, they could be left blank).

4.2.3 Activation

The activation process, as described before in comparison to procurement, is mainly devoted to the definition and dissemination of operation schedules and settings for the next market periods.

As defined here, schedules refer to active power versus time commitments resulting from economic market clearance and technical constraint resolution. The idea behind settings is that the parameter is defined by the system operator according to the outcome of the network analysis process (no market). In our use cases, the latter affects mainly voltage and droop settings.

The first steps of the use case are common for all coordination schemes. Only scenario 2 has a specific path that allows blocking of some of the bids by the DSO, based on previously communicated market outcome (last step of procurement phase). This is applicable to CSs A and E.

Those CSs with local market structures have dedicated communication requirements. An additional optional path results from the fact that CMPs may need to calculate/translate aggregated schedule or settings to individual DER asset settings.

Again, DSOs in CS B are considered as CMP.

All this aspects are presented in the next activity graph.

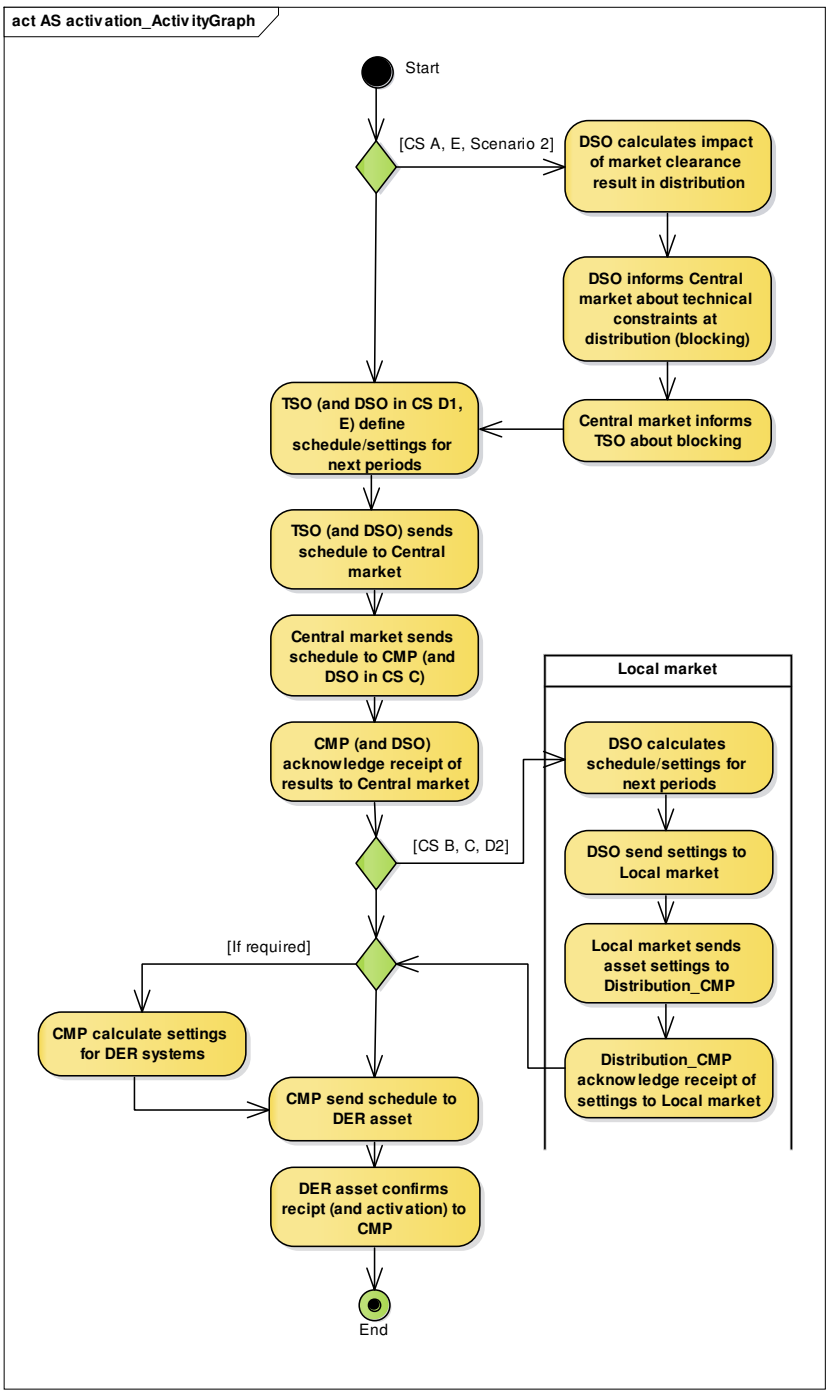


Figure 4.7 Use Case activation process activity graph

From these steps the following data models can be derived:

- **Blocking message**: it should indicate the affected area/node in the distribution network for each blocked bid.
- **Schedule/Settings message**: the schedule message refers to the final results obtained from the market clearing plus the technical contingency resolution process (schedule for the next

market steps). This message is expected to have the same fields of information as the market results message. It is valid for both central and local markets, and it may use the same format from the TSO to the final DER (content may change: aggregated versus DER asset specific data). The settings message can be similar to the schedule message. Since results do not come from a market setting but from own system operator calculations, the reference to market sessions is not necessary, in this last case.

- **Acknowledgement message**: schedule/setting receipt confirmation message. As mentioned before, it could have a common structure in all cases (e.g. time stamp and some reference to the received message).

4.2.4 Settlement

This process deals with the assessment of the commitment fulfilment by service providers and with the financial settlement derived from it.

As mentioned above, the settlement process is not so directly linked to the common day-ahead or intraday market processes, especially the financial assessment. With regard to the assessment of commitments fulfilment, system operators need to collect network measurements to analyse the real performance of service providers. This activity is a common process linked to their real time systems (e.g. SCADA, EMS, DMS) and, therefore, main steps are common to all AS use cases. Market related specific tasks are the selection and preparation of data to be sent to the market operator, who checks the acquired commitments against the real performance of CMP systems, in order to perform the financial settlement. This financial settlement, which ends with the monetary exchange, is completed in longer time periods (e.g. one month).

As proposed in the next activity graph (Figure 4.8), one settlement per market (central and local) should be performed.

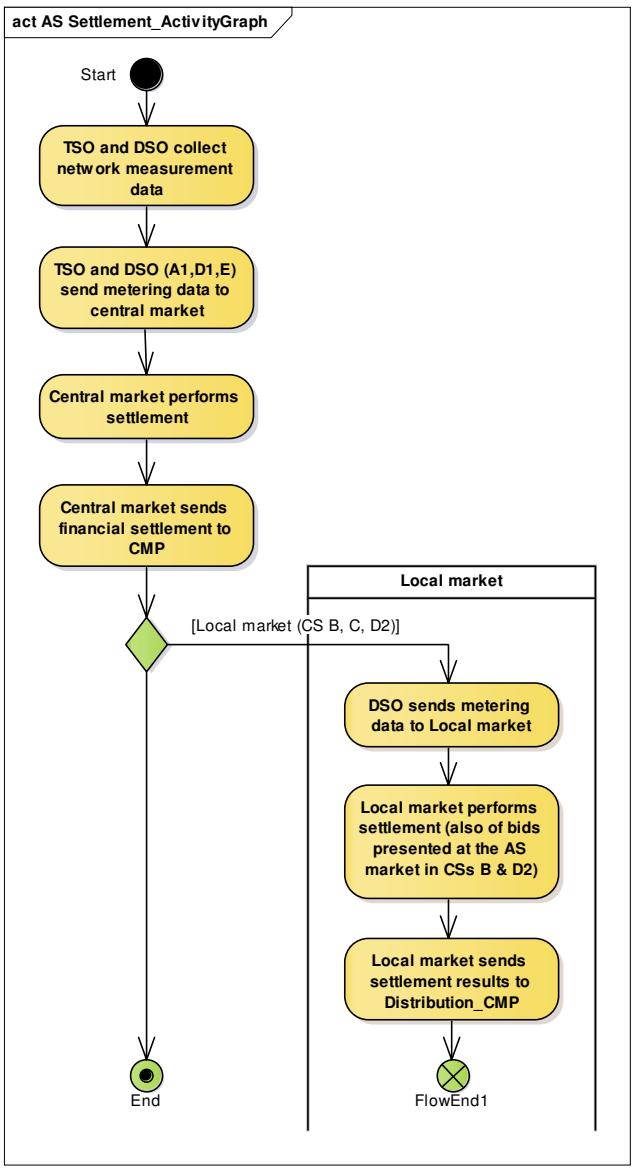


Figure 4.8 Use Case settlement process activity graph

The data models linked to this process are those related to the communication of network parameter measurements and of the financial settlement:

- **Measurement messages**: this message should send the data permitting the market operator assess the commitment fulfilment by flexibility service providers. Even if each use case refers to specific services, the network parameters to be considered will be normally common to all of them (voltage, current, active and reactive power...). This permits to use a common message format for all of them. Data models could be common for distribution and transmission networks, even if not all fields might be applicable or meaningful for both systems and could be left blank.

- **Financial settlement message**: this message should contain information about the bid ID, the main commitments acquired in that bid, the measurements performed by the system operator (those related to the specific CMP performance) and the economic results derived from them. The message format could be common for central and local market environments.

4.3 Market design

Market design has also implications on ICT requirements. The main characteristics of the SmartNet market described in [2], i.e. bidding, timing, clearing and pricing, have all implications on ICT. It is important to remember that this market is focused on the procurement and activation processes and on active power trade (UC 1 and UC 2).

Locational nodal **pricing** sets the need to include node information on bids and, therefore, it affects data models.

Regarding **bidding**, three main bid types are defined in the SmartNet market ([2]):

- **UNIT-bids**: it is defined for a time step by a price (P0) and quantity (Q0). Three subtypes are considered:
    - **Non-curtailable unit bid**: it has one price for one quantity, which can be both positive and negative. The information contained in the bid definition must be the following:

      BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, STEP, NON_CURTAILABLE, POWER_FACTOR, Q0, P0

    - **STEP curtailable unit bid**: it has a single price (P0) for a range between two quantities (Q0-Q1). The data contained in the bid message must be the following:

      BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, STEP, CURTAILABLE, POWER_FACTOR, Q0, P0, Q1

    - **PWL (piecewise linear) curtailable unit bid**: it has a linearly variable marginal price (P0-P1) for a range between two quantities (Q0-Q1). The bid must consist of the following fields:

      BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, PWL, CURTAILABLE, POWER_FACTOR, Q0, P0, Q1, P1

- **Q-bids**: they are like UNIT-bids but they provide longer vectors of quantities and prices (P0, P1, P2, P3..., Q0, Q1, Q2, Q3...). The objective is to allow a direct expression of an aggregated curve of flexibility with varying marginal cost. The same subgroups as above apply and they can be defined as follows:

- BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, STEP, NON_CURTAILABLE, POWER_FACTOR, Q0, P0, Q1, P1...QN-1, PN-1
- BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, STEP, CURTAILABLE, POWER_FACTOR, Q0, P0, Q1, P1...QN-1, PN-1
- BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, PWL, CURTAILABLE, POWER_FACTOR, Q0, P0, Q1, P1...QN-1, PN-1

- **Qt-bids:** they offer a Q-bid for a series of time steps within the window of optimization and allow expressing in advance the availability of flexibility for the future time steps. Inter-temporal constraints can be added. The subgroups above are specified as below:
  - BID_ISSUER_ID, BID_ID, NETWORK_NODE_ID, UNIT_BID, STEP, NON_CURTAILABLE, POWER_FACTOR, t=0, Q0, P0, Q1, P1...QN-1, PN-1, t=1, Q0, P0, Q1, P1...QN-1, PN-1... t=11[10], Q0, P0, Q1, P1...QN-1, PN-1)
  - Similarly to the previous one.

Additional **optional information** might be included in the bid if needed (integrated in the same message or in a separate message with the same BID_ID):

- **Intra-bid temporal constraints**: "Accept-All-Time-Steps-or-None"; ramping constraints (MAX_RAMP_UP_PER_STEP = N, MAX_RAMP_UP_PER_STEP= N); maximum number of activations (X) over a time horizon (Y) (MAX_N_ACTIVATIONS_PER_STEPS = (X,Y); minimum and maximum duration of an activation in terms of number of time steps (MIN_N_STEPS_PER_ACTIVATION = N, MAX_N_STEPS_PER_ACTIVATION = N); minimal duration between two activations; and integral constraint (integral of generation over a set of market sessions).
- **Inter-bid logical constraints**: implication constraint (select a bid only if another bid has been accepted as well), e.g. BID_ISSUER_ID=100.101.102.1, IMPL_ACCEPT, BID_ID=22, BID_ID=21; exclusive choice constraint (exclusive acceptance between a set of bids), e.g. BID_ISSUER_ID=100.101.102.1, EXOR_ACCEPT, BID_ID=22, BID_ID=7, BID_ID=8, BID_ID=30; deferability constraint (maximum delay in acceptance in terms of time steps), DEFERABILITY = Max.

Timing is an important feature of the market. The integrated reserve is a discrete/closed-gate market, cleared frequently (e.g., 5 minutes) and using a rolling optimization (e.g. 1 hour). The clearing frequency, 5 minutes, sets a time limit requirement for all communications and computational steps to be performed

[10] t=0 to t=11 meaning the 12 five minute steps in one hour horizon (considering these assumptions).

within each market session. The tasks that should fit within this time gate are described in the procurement and activation processes presented in the previous subsection (0 and 4.2.3):

- **Computation time**: it is mainly devoted to economic market clearance and technical constraint resolution tasks.
- **Communication time**: the maximum available time for message exchange is the market clearance step (e.g. 5 minutes), minus the time required for computation. This remaining time sets maximum latency requirements for messages. It should be considered that some messages, e.g. acknowledgement messages, do not block the sending of other messages, i.e. they can be sent in parallel; while others need to wait for some previous message before they can be forwarded (series processing). This should be considered to determine the maximum latency available for each message. In a more accurate assessment, possible delays related to quality of service issues should also be taken into account.

Clearing characteristics of the SmartNet market also affect ICT requirements. The approach considered in the procurement and activation processes above, just in the boundary between them, is conventional: economic clearance and technical constraints are performed by different business actor roles, i.e. market and system operator. However, in the SmartNet market, the algorithm clearing the market considers at the same time both technical constraints and economic aspects of bids. This has two main implications with respect to the previous approach:

- The market operator should have almost as much information of the grid as the system operator. This would result easier when both roles are played by the same actor, which is indeed true for most CSs in SmartNet, and when market economic aspects are fully integrated in system operator's non-real time backend systems, i.e., this would require a major integration of two roles that today are independent. In the case of CS E, an independent market operator should possess, understand and manage the data of distribution and transmission networks. This may involve issues related to confidentiality of sensitive data, responsibility of network operation, etc., which should be clearly specified by the regulation. In addition, the way to transmit network information between system operators and the IMO should be also specified.
- In regard to the steps proposed in the integrated use case description, some could be avoided in the activation process:
    - TSO (and DSO) define schedule/settings for next periods: this computation task would be added to the step in procurement dealing with market clearance.
    - TSO (and DSO) sends schedule to central market: no need for this message exchange.

5 SmartNet pilot and simulation requirements

The feasibility of the SmartNet framework is tested in the project through three complementary means: simulations, technological pilots and laboratory tests.

In the first part of this section, the focus is set on the technological pilots. The ICT requirements of those pilots are gathered and evaluated against the more generic ICT requirements captured from coordination schemes, use cases and SmartNet market introduced in the previous sections. The aim of technological pilots is to demonstrate that technology is readily available and to identify potential issues or barriers for the field implementation of the solutions proposed in SmartNet. On the contrary, simulations and laboratory tests are aimed at assessing the potential benefits of SmartNet solutions in the future (2030). As a result, some of the technologies described in this deliverable, which are expected to be fully operational in 2030, cannot be tested in the pilots, due to their present status of development. In the project, this affects especially the interaction of the pilot actors with the market, which is under development, and includes features that cannot be found in current market designs. As consequence, at this stage, the description of the pilots is more focused on network operation solutions.

In the last subsection, the characteristics of the laboratory setup for the SmartNet project are presented. The laboratory tests, together with the simulations, provide higher levels of flexibility to assess the solutions proposed in the project.

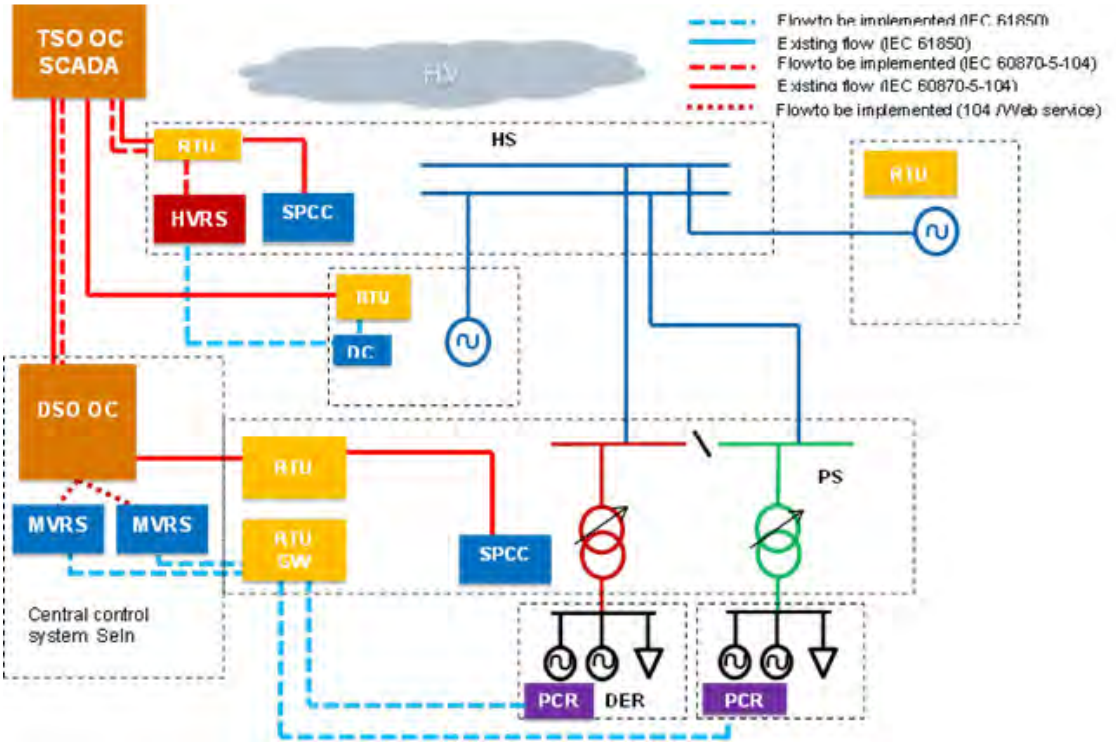
5.1 Italian pilot (Pilot A)

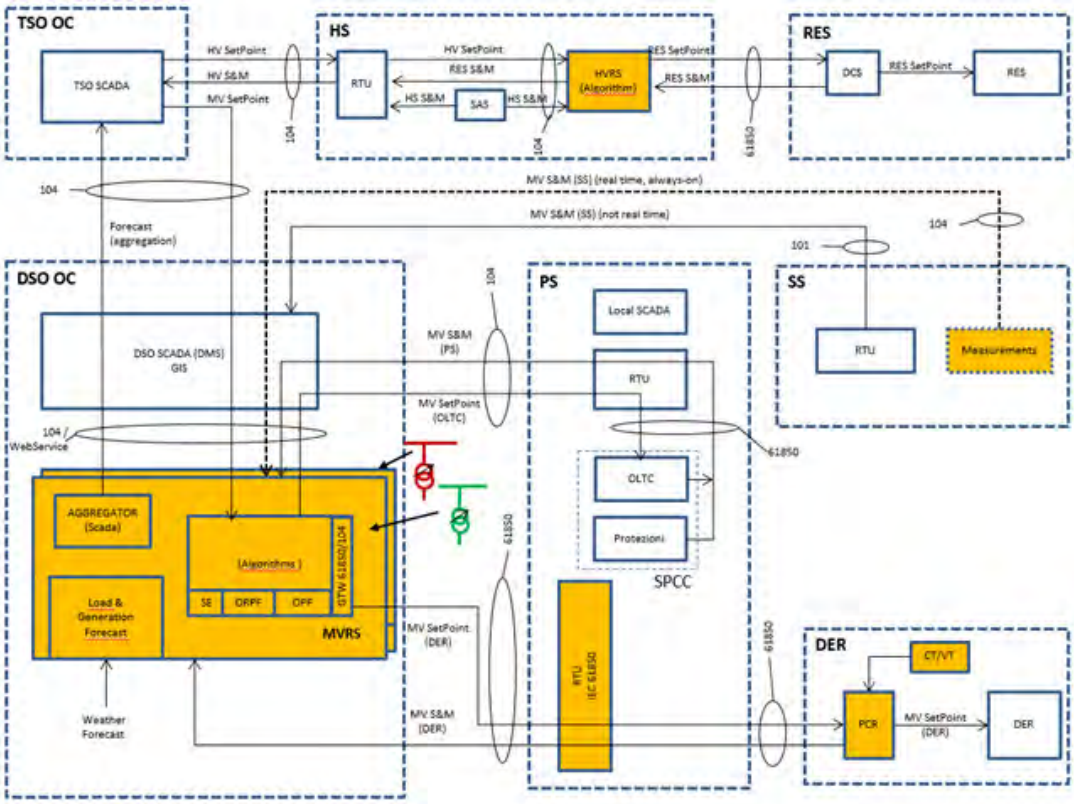
5.1.1 ICT characteristics description

Pilot A aims at implementing three main functionalities:

- **Advanced monitoring of MV network**: each 20 seconds, the sum of load and generation will be measured for the grid connected at each HV/MV transformer.
- **Balancing**: large size Renewable Energy Source (RES) generators connected to the HV network will provide active power.
- **Reactive power support**: DERs connected at medium voltage will provide dynamic capability and will react to reactive power set points on MV busbar. The response is expected to happen in minutes.

The general and detailed schemes deployed for the pilot are presented in the figures below. Here, the main components and the communication links among them are specified.


TSO OC SCADA
HV
Flowto be implemented (IEC 61850)
Existing flow (IEC 61850)
Flowto be implemented (IEC 60870-5-104)
Existing flow (IEC 60870-5-104)
Flowto be implemented (104 /Web service)
HS
RTU
HVRS
SPCC
RTU
DC
RTU
DSO OC
RTU
MVRS
MVRS
RTU SW
SPCC
PS
Central control system Sein
PCR
DER
PCR


TSO OC
TSO SCADA
HV SetPoint
HV S&M
MV SetPoint
104
HS
RTU
HV SetPoint
RES S&M
HS S&M
SAS
HS S&M
HVRS (Algorithm)
RES SetPoint
RES S&M
104
61850
RES
DCS
RES SetPoint
RES
104
Forecast (aggregation)
MV S&M (SS) (real time, always-on)
MV S&M (SS) (not real time)
104
101
DSO OC
DSO SCADA (DMS) GIS
104 / WebService
AGGREGATOR (Scada)
(Algorithms)
SE
ORPF
OPF
GTW 61850/104
Load & Generation Forecast
MVRS
Weather Forecast
MV S&M (PS)
MV SetPoint (OLTC)
MV SetPoint (DER)
MV S&M (DER)
104
61850
61850
PS
Local SCADA
RTU
OLTC
Protezioni
SPCC
RTU IEC 61850
SS
RTU
Measurements
61850
DER
CT/VT
PCR
MV SetPoint (DER)
DER

Legend	
Acronym	**Description**
TSO OC	TSO Operation Centre
DSO OC	DSO Operation Centre
HS	HV Substation
PS	Primary Substation
SS	Secondary Substation
RES	HV Generation/Customer
DER	MV Generation/Customer
SPCC	Substation Local protection, command and control system
SAS	Substation Automation System
RTU	Remote Terminal Unit
OLTC	On Line Tap Changer
PCR	Plant Central Regulator (interface between power generation module control system and MVRS)
HVRS	High Voltage Regulation System (device which performs functions and algorithms for the aggregation and the control of generation at high voltage level)
MVRS	Medium Voltage Regulation System (device which performs functions and algorithms for the aggregation and the control of dispersed generation)
S&M	State & Measures
CT/VT	Current/Voltage Transformers

Figure 5.1 Pilot A general (top) and detailed schemes (and legend table)

The communication technologies and information types that are adopted in the pilot are presented in the table below for each of the relevant interfaces identified in the previous figure (interface acronyms are based on the legend of Table 5.1).

Interface	**Communication tech.** **Type (T) protocol stack (P)**	**Information type**
SCADA (TSO) - RTU (HS)	*T*: public cellular network *P*: 3G/4G	*T*: HV set points, HV state & measures *P*: IEC 60870-5-104
RTU (HS) - HVRS (HS)	*T*: wired? *P*: ?	*T*: HV set points, RES state & measures *P*: IEC 60870-5-104
HVRS (HS) - RES OC	*T*: public cellular network *P*: 3G/4G	*T*: state & measures, P set point *P*: IEC 61850
OC (RES) - RES	*T*: wired? *P*: ?	*T*: state & measures, P set point *P*: proprietary?
SCADA (TSO) - MVRS (DSO)	*T*: public cellular network *P*: 3G/4G	*T*: MV aggregation forecast (20 s), MV set point *P*: IEC 60870-5-104
MVRS (DSO) - RTU (PS)	*T*: public cellular network *P*: 3G/4G	*T*: MV set point, MV state & measures *P*: IEC 60870-5-104
RTU (PS) - SPCC (RTU)	*T*: wired? *P*: ?	*T*: MV set point, MV state & measures *P*: IEC 61850
MVRS (DSO) - RTU (SS)	*T*: public cellular network *P*: 3G/4G	*T*: MV state & measures (not real time) *P*: IEC 60870-5-101
MVRS (DSO) - Measurement system (SS)	*T*: public cellular network *P*: 3G/4G	*T*: MV state & measures (real time) *P*: IEC 60870-5-104
MVRS (DSO) - PCR (DER)	*T*: public cellular network *P*: 3G/4G	*T*: state & measures, Q set point *P*: IEC 61850

Interface	Communication tech. Type (T) protocol stack (P)	Information type
PCR (DER EMS) - DER	*T*: wired? *P*: *?*	*T*: state & measures, Q set point *P*: proprietary?

Table 5.1 ICT requirements for Pilot A

5.1.2 Assessment from SmartNet approach

Two SmartNet UCs and CSs are considered in this pilot:

- **UC2** (balancing and congestion management): it is linked to the balancing functionality above. It adopts the **coordination scheme A** (central dispatch), variant 2 (the TSO monitors the DSO network), and scenario 3 (DSO sets distribution network constraint in the market clearing process).
- **UC3** (voltage control): it refers to the reactive power support service above. The TSO-DSO relationship follows **coordination scheme C** (the TSO establishes set points to be followed by the DSO) and scenario 3.

Figure 5.1 presents the communications at network level but the links with the market are not included. In general, the communications seem to respond to real time monitoring and operation activities, which even if necessary for an efficient operation of smart grids, they are not included in the SmartNet AS use cases description, where the focus is set on market related communications.

According to the proposed approach in the previous sections, the information exchange related to AS procurement and activation (including settings) should be performed through the market platform, i.e. messages from the system operator (TSO) to the grid operator (DSO) or service providers (CMP) should go through the market operator, and this is not clear in the previous figure, where the control of assets seems to be centralised, even for DER. Under market schemes, DER owners (flexibility providers) activate their assets as response to market clearance results. We could consider that, instead of roles, the figure considers parties and, then, the TSO would be both system and market operator and, therefore, responsible for transmitting market messages. This interpretation of the scheme would fit better with CS A business case, although the participation of distribution network aggregators in the AS market is not considered, which is the most innovative aspect about CS A. The solution to interface with the market proposed in this pilot is not clear, but seems to be in line with current approaches, which pivot on the system operator.

Regarding monitoring, SmartNet CS A defines variant 2, which proposes that the TSO monitors directly DSO data. In this sense, the pilot is in line with the project approach. Generally speaking, if possible in theory, the way to implement this option is quite challenging. Unless both system and distribution grid operators are the same party, which is not common throughout Europe, confidentiality, security, business competition and other issues are easy to arise under this variant. Apart from this, it

remains to be seen how monitoring can be technically performed: does the DSO send real time measures to the TSO? This requires a continuous transfer of big amounts of information when high number of DERs are involved; would the TSO build monitoring systems in parallel to those of the DSO? If so, where? In DSO installations?; etc. In addition, it must be considered that if the TSO controls directly DER assets at distribution, this may not cause always the same targeted impact at transmission border nodes, since distribution network characteristics (e.g. transformer tap changers, condenser banks, topology...) may be changed by the DSO. Also from the business level point of view, network operation responsibilities and business model related aspects may require a deep revision under this scheme. Therefore, a completely new set of rules, including ICT requirements, would have to be defined to permit such a monitoring and control approach. However, and as mentioned before, this part is not considered, at least in detail, in SmartNet UCs.

Regarding specifically the reactive power support (UC 3), apart from the central market issues mentioned before, a local market is also foreseen under coordination scheme C, and this is not mentioned in the definition of the pilot. It would be reasonable to consider a mix of CS C and A, in which the TSO sends settings to DSOs and this responds without the use of a local market, but this leads to a conventional case today (no innovative approach).

The proposed communication technologies and information protocols are in line with the EU approach as described in sections 9 and 10. The communication between TSO and DSO seems to respond to inter-control centre networks, even if the proposed protocol for data exchange (IEC 60870-5-104) is not the specific one for that purpose (see Table 10.1).

5.2 Danish pilot (Pilot B)

5.2.1 ICT characteristics description

The main scope of SmartNet Pilot B is to show how a basic Demand Response (DR) system can benefit both summerhouse owners', local DSO's interests and national energy balancing. The deployed system seeks the optimal use of energy through the regulation of the water temperature in the houses' pools.

Three main **interfaces** (A, B and C) have been considered so far for the information exchange:

A. **Inside summerhouses**: interface between the sensors, heating, power and the controllers.
B. **Between house and aggregating system**: interface between the summerhouse controllers and the technical aggregating system (gateway).
C. **Between aggregating system and backend**: interface between the technical aggregating system and the central control for Demand Response.

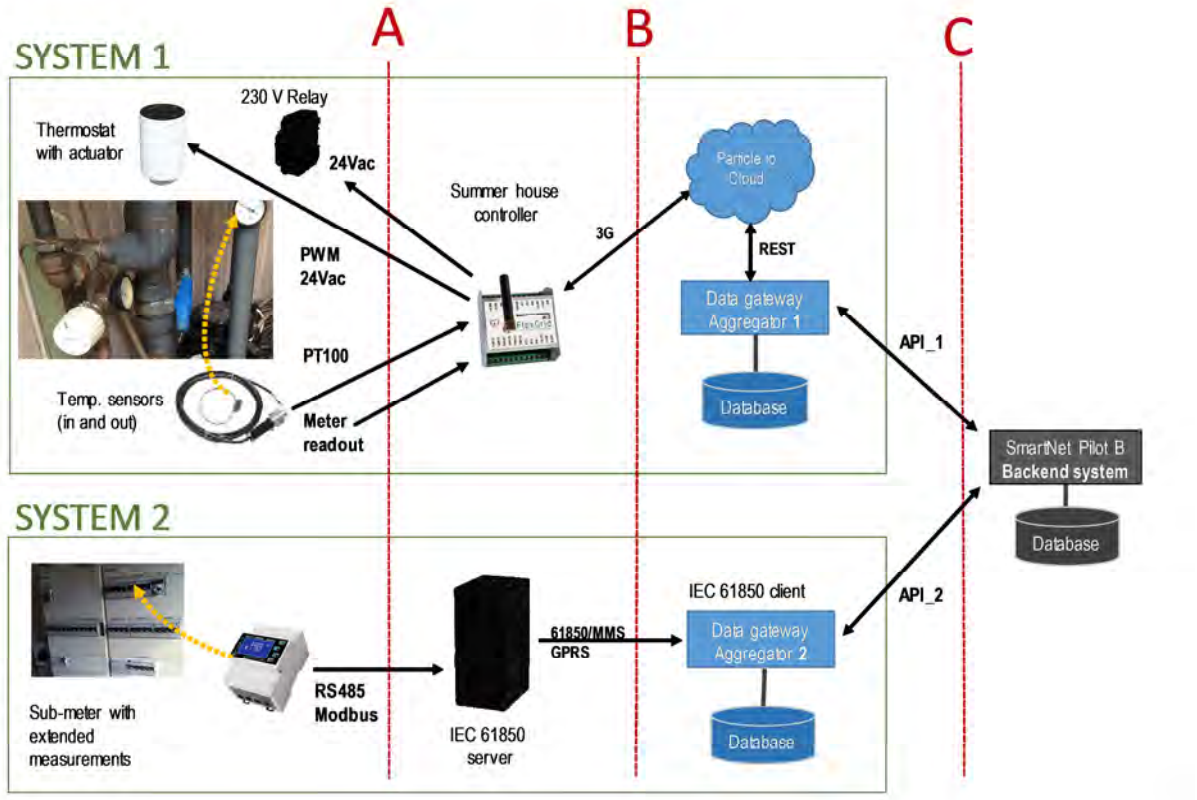


Figure 5.2 Pilot B interfaces

Some of the characteristics of the of the temperature **control system** are the following:

- The loop frequency from backend system to summerhouse controller is expected to be 5 minutes, but this is one of the findings that is to be revealed during the Pilot tests.
- The "set-point signal" is basically the temperature that is expected in the pool (ranging from 10°- 31°C).
- On average it takes 24 hours to raise the temperature 3°C in the pool.

The **general requirements** of the system are the following:

- The pool pump must never be switched off when there are people using the summerhouse.
- The pool pump must never be switched off when the heat exchanger or heat booster is running.
- The water temperature in the pool must always be between 27°-29°C, when it is rented out. However, during night hours (22:00 to 8:00) it may be slightly higher.
- The air temperature in the pool area must always be 2°-3°C above the pool water temperature.
- The dehumidifier inside the pool area must never be switched off.

Some more **specific implementation requirements** for the main systems in Figure 5.2 are described below:

- **SYSTEM 1:**
  - All measured values, status values, alarms and set-points must include a timestamp, with the time zone set to UTC. Timestamps must be based on a clock that is synchronised to, at least, one server in the dk.pool.ntp.org NTP server cluster.
  - Temperature for water flowing into the pool ("Temp Water in") and out of the pool ("Temp Water out), and room temperature ("Temp Air") must be measured and timestamped in 5 minute intervals (i.e. at minute 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55 within the hour).
  - "Temp Water in", "Temp Water out", "Temp air" and their timestamp must be sent to the "Data Aggregator 1" every 5 minute (i.e. at minute 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55 within the hour).
  - If the temperature in the room ("Temp air") is 3 degrees or more below the "Temp Water in", then a status signal ("Temp warning 1") must be sent to "Data Aggregator 1".
  - The set-point temperature must be checked every 5 minutes and, if changed since the last check, SYSTEM 1 controller must be updated.
  - The summerhouse controller must change the $24V_{AC}$ Pulse Width Modulation (PWM) signal on the thermostat according to the newest set-point value every 5 minutes.
  - The summerhouse controller must switch the 230 V relay off if the signal "Relay" is "0", and on if the signal "Relay" is "1".
  - The summerhouse controller must always check if the "Temp Water in" is higher than "Temp Water out" when the pool pump (Relay) is switched off. If the "Temp Water in" is higher than "Temp Water out", then a "Temp warning pump" must be signalled.
  - The summerhouse controller must always check if the booking status is "occupied" or "free". If "occupied" the pool pump "Relay" must never be switched off.
  - The summerhouse controller must always check if the booking status is "occupied" or "free". If "occupied" the pool temperature must be between 27°-29°C.
  - All sensors must be main supplied (no batteries).
- **SYSTEM 2:**
  - All measured values must include a timestamp, with the time zone set to UTC. Timestamps must be based on a clock that is synchronised to, at least, one server in the dk.pool.ntp.org NTP server cluster.

- Information according to the measurement requirements for SYSTEM 2, must be acquired by the IEC 61850 server via the measurement unit (wired M-bus), timestamped and stored as a MMXU Logical Node (LN) according to the IEC 61850 standard.
- Data must be acquired and timestamped every 5 minute (i.e. at minute 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55 within the hour).

- **Data Gateway Aggregator 1:**
  - All timestamps must have their time zone set to UTC. Timestamps must be based on a clock that is synchronised to, at least, one server in the dk.pool.ntp.org NTP server cluster.
  - All status and measured values received from SYSTEM 1 must be stored as received (i.e. keeping all received information intact), with an additional received-at timestamp. The aggregator must check that values are received every 5 minute (i.e. at minute 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55 within the hour) and set an alarm if this is not the case. This alarm must be readable by aggregator clients via a well-defined and well-documented API.
  - The aggregator must act as a server, making all received values available at any given time to an aggregator client. Access to the data on the server must be provided by a well-defined and well-documented API.
  - The aggregator must act as a server, allowing an aggregator client to send set-points and command signals via a well-defined and well-documented API.
  - The aggregator must have an uptime of at least 99%, measured on a monthly basis (equals a downtime of max. 7 hours every month).

- **Data Gateway Aggregator 2:**
  - All timestamps must have their time zone set to UTC. Timestamps must be based on a clock that is synchronised to, at least, one server in the dk.pool.ntp.org NTP server cluster.
  - The aggregator must read measured values from SYSTEM 2 every 5 minute (i.e. at minute 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50 and 55 within the hour). Values must be stored as read (i.e. keeping all received information intact), with an additional received-at timestamp.
  - The aggregator must act as a server, making all measured values available at any given time to an aggregator client. Access to the data on the server must be handled by a well-defined and well-documented API.
  - The aggregator must have an uptime of at least 99%, measured on a monthly basis (equals a downtime of max. 7 hours every month).

The **signal lists** of the two systems are shown in the next tables.

SYSTEM 1			
Information name	**ID**	**Type**	**Unit**
Pool water temperature into the pool	Temp Water in	Measurement	Degrees C
Pool water temperature out of the pool	Temp Water out	Measurement	Degrees C
Pool area air temperature	Temp area in	Measurement	Degrees C
Electrical meter (current meter value)	Meter value	Measurement	Kwh
Temperature warning pool room	Temp warning room	Status	Degrees C
Temperature warning pool pump	Temp warning pump	Status	Degrees C
Booking status	Booking	Status	Boolean
Temperature set-point	Temp set point	Set-point	Degrees C
230 V relay to switch pool pump off and on	Relay	Control	Boolean

Table 5.2 System 1 signal list

SYSTEM 2			
Information name	**ID (IEC 61850, MMXU LN)**	**Type**	**Unit**
Active power from phase A	MMXU1.W.phsA.cVal.mag.f	Measurement	W
Active power from phase B	MMXU1.W.phsB.cVal.mag.f	Measurement	W
Active power from phase C	MMXU1.W.phsC.cVal.mag.f	Measurement	W
Active power from neutral	MMXU1.W.neut.cVal.mag.f	Measurement	W
Reactive power from phase A	MMXU1.VAr.phsA.cVal.mag.f	Measurement	VAr
Reactive power from phase B	MMXU1.VAr.phsB.cVal.mag.f	Measurement	VAr
Reactive power from phase C	MMXU1.VAr.phsC.cVal.mag.f	Measurement	VAr
Reactive power from neutral	MMXU1.VAr.neut.cVal.mag.f	Measurement	VAr
Voltage from phase A	MMXU1.PNV.phsA.cVal.mag.f	Measurement	V
Voltage from phase B	MMXU1.PNV.phsB.cVal.mag.f	Measurement	V
Voltage from phase C	MMXU1.PNV.phsC.cVal.mag.f	Measurement	V
Voltage from phase neutral	MMXU1.PNV.neut.cVal.mag.f	Measurement	V
Frequency (50 Hz)	MMXU1.Hz.mag.f	Measurement	Hz
Power factor from phase A	MMXU1.PF.phsA.cVal.mag.f	Measurement	Cos phi
Power factor from phase B	MMXU1.PF.phsB.cVal.mag.f	Measurement	Cos phi
Power factor from phase C	MMXU1.PF.phsC.cVal.mag.f	Measurement	Cos phi
Power factor from phase neutral	MMXU1.PF.neut.cVal.mag.f	Measurement	Cos phi

Table 5.3 System 2 signal list

The next table sums up the ICT information for this pilot at the current status of definition. Type (T) and protocol stack (P) of communication and information are provided when available.

Interface	Communication tech. Type (T), Protocol stack (P)	Information type
System 1		
Thermostat-Controller	*T*: wired *P*: PWM	*T*: temperature set point *P*: PWM
Temperature sensors - Controller	*T*: wired *P*: - (analogue signal: PT100)	*T*: temperature measurement *P*: - (analogue signal: PT100)
Relay - controller	*T*: wired *P*: - (analogue signal: 24VDC)	*T*: on/off signal *P*: - (analogue signal: 24VDC)
Meter - controller	*T*: wired *P*: M-bus	*T*: current measurement *P*: M-bus
Controller - data aggregator 1	*T*: public cellular network *P*: REST	*T*: Status, measurement *P*: REST
Data aggregator 1- backend system	*T*: Internet (IP) *P*: REST	*T*: Status, measurement *P*: REST/JSON
System 2		
Submeter - IEC 61850 server	*T*: wired (RS 485) *P*: Modbus	*T*: measurement *P*: Modbus
IEC 61850 server - data aggregator 2	*T*: public cellular network *P*: GPRS	*T*: measurement *P*: IEC 61850/MMS
Data aggregator 1- backend system	*T*: Internet (IP) *P*: REST	*T*: measurement *P*: REST

Table 5.4 ICT requirements for Pilot B

5.2.2 Assessment from SmartNet approach

From ICTs point of view, the previous subsection is focused on the asset control up to the aggregator level, but no detailed information is given on market interaction aspects, which seem to be currently under definition. The comments made for Pilot A to this respect are also applicable here.

SmartNet UC2 is considered in this pilot under coordination scheme D (common TSO-DSO market model). As mentioned before, it remains to be defined if the joint work between TSO and DSO would be materialised in a new market actor depending on both DSO and TSO parties. This scheme would be similar to CS E, where the new actor would play the role of the IMO. If not, the information exchange between the TSO and DSO devoted to rule the common market should be clearly established, together with the responsibilities of each of them in the shared role of market operator. In this case, CIM standards (IEC 61968, IEC 61970) should be regarded as main reference.

For system 1, control and measurement loop is executed once every five minutes. Therefore, if the market clearing frequency is assumed to last also for five minutes, the visibility of network assets would be limited. This reduces the flexibility of the aggregated assets and involves increased challenges for the CMP to participate in the procurement and activation processes of short period window markets. It

should be checked whether this handicap could be balanced by the use of models describing the behaviour of the flexible assets.

The capacity of aggregation is an additional challenge for the CMP in this case, because the flexibility that can be provided by each asset is limited due to the size of the equipment (pool pump). However, it must be considered that assets like these in Pilot B would only be part of the total pool of DER resources that the CMP would use for market interaction.

In system 2 and from the IEC 61850 server upstream, the proposed communication technologies and information protocols are in line with the EU approach as described in sections 9 and 10. Regarding system 1, the aggregation of measurements does not seem to follow a standardised data model. Nevertheless, at end devices level (field and process zones), especially when they are simple systems, it is common to find de-facto standards based on simpler communications.

5.3 Spanish pilot (Pilot C)

5.3.1 ICT characteristics description

In pilot C, the DSO (Endesa) will buy flexibility capacities from two main providers that aggregate DER connected at the distribution network. The DSO uses this flexibility, related to active power and voltage control, to follow the set points established by the TSO (CS C). The following main roles are involved in the pilot:

- Aggregator of mobile telecom radio base stations (ONE): portfolio of 50 kW of flexibility from radio base stations. Base stations are owned by Vodafone who plays the role of DER owner.
- e-Mobility infrastructure operator (CSO) and e-Mobility service provider (EMSP): these roles are played by Endesa and 100 kW are aggregated. They are available from Electric Vehicles (EV), which are able to charge and supply energy to the network using Vehicle to Grid (V2G) technologies.

The following figure shows the general architecture of pilot C.

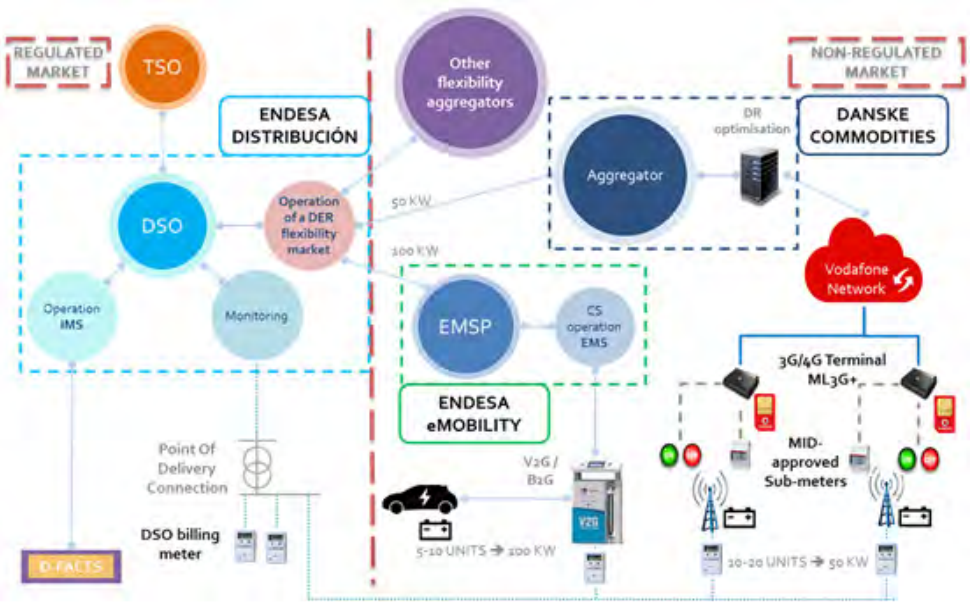


Figure 5.3 Pilot C general architecture

The next table shows the communication technologies and main information characteristics for the provision of network services in Pilot C, at the current state of development. Features are given for each main interface involved, following the architecture shown above and according to the services that need to be provided. Type (T) and protocol (P) of communication and information are given when available.

Interface	Communication tech.	Information type
EV - EVSE (EV Supply Equipment)	*T*: wired through EV connector *P*: CHAdeMO	*T*: Power setting *P*: CHAdeMO v2
EVSE - EMSP backend (CS operation)	*T*: wireless *P*: LoRa/NB-IoT	*T*: Power settings *P*: proprietary (EMMS)
EMSP - DSO market	*T*: public cellular network? *P*: 3G/4G?	*T*: power settings, prices (day-ahead), service activation message (DSO) *P*: ?
Batteries - Local controller	*T*: wired? *P*: Modbus	*T*: on/off Protocol: Modbus
Batteries Submeter - Local controller	*T*: wired? *P*: Modbus	*T*: measurements *P*: Modbus
Local controller - Aggregator backend	*T*: cellular, secure APN *P*: 3G/4G	*T*: on/off, measurements (every minute) *P*: ?
Aggregator - DSO market	*T*: public cellular network? *P*: 3G/4G?	*T*: power settings, prices (day-ahead), service activation message (DSO) *P*: ?
DSO - TSO	*T:* Internet *P:* Web services	*T*: Market signals (price...) *P*: Proprietary (TSO defined)

Table 5.5 ICT requirements for Pilot C

For the EVSE - EMSP backend (CS operation) communication path, and specifically for the V2G segment, an extensive analysis on IoT technologies must be carried out in the pilot. In regards to the IoT technologies that will be considered, NB-IoT must be separated from other technologies like SigFox and LoRa. The reason for such differentiation comes from the fact that, at this moment, many mobile operators have set up dedicated IoT/M2M business units in order to serve the growing demand and the only standardized solution currently available is NB-IoT.

When inherent capabilities of NB-IoT are compared with other Low Power WAN (LPWAN) technologies like eMTC, SigFox, and LoRa (see 9.2), NB-IoT offers better performance, since it guarantees 20+dB coverage, around 1000x connections and, approximately, 10 years, using only 200 kHz bandwidth. Looking at all the technologies in terms of network investment, coverage scenario, uplink and downlink traffic, and network reliability NB-IoT is the most suitable technology. Additionally, from a performance point of view, NB-IoT has been already standardized (June 2016) and therefore holds a quite an extensive ecosystem mainly because of its support from many global top operators. The most important difference when compared to unlicensed solutions (e.g. SigFox and LoRa) is that these cannot guarantee reliability and security.

5.3.2 Assessment from SmartNet approach

Pilot C arrangement relates to coordination scheme C (the TSO establishes set points for the DSO to meet them). In order for the DSO to fulfil the scheduled exchange program, it needs to make use of balancing capabilities at distribution network level, which are traded at a local DER flexibility market.

In this pilot, two SmartNet UCs are considered under CS C: 2 (balancing and congestion) and 3 (voltage control). Scenario 3 (DSO sets distribution network constraints in the market clearing process) is considered for both UCs.

Pilot C approach fits to SmartNet UC and CSs description.

Regarding the communication technologies and information protocols, the following comments are made when compared to the EU approach described in sections 9 and 10:

- The preferred option in Europe for the EV - EVSE link to provide fast charging is the Combo Charging System (CCS), but CHAdeMO is widely deployed and used.
- Modbus is a much extended de-facto standard but is not among those selected by the SG-CG for smart grids.
- NB-IoT is a Low Power Wide Area communication technology (see section 9.2) linked to the Internet of Things (IoT) applications, which are becoming more and more important. It presents a good performance in terms of coverage (which helps getting metering data from remote sites), low power consumption and massive deployments. Few of the standards related to IoT are considered today in the list of those proposed by the SG-CG for

interoperable smart grids across Europe, but this may change in the future with the increased deployment of these standards. Pilot C is a good opportunity to test this technology.

- Communications with the market platform in Spain are performed using a proprietary (TSO defined) protocol. For the sake of interoperability, proprietary solutions should evolve towards the standards proposed at the EU level. However, this involves great impact in current systems, leading to long deployment time.

5.4 Laboratory test and simulations

Due to the inherent features of their systems, real life pilots have limitations to test new innovative approaches. By contrast, simulations provide enough flexibility to go beyond current network and market deployments. In between both, flexible laboratory environments make possible to test the behaviour of real devices in configurations that do not have to be close to real operation, which are achieved through simulation and emulation.

The simulations and laboratory tests in SmartNet will focus on validating the technical feasibility of the coordination schemes that could not be implemented in the technological pilots.

As mentioned above, simulations permit a higher level of flexibility to test different market and network configurations, however, the flexibility of laboratory tests is linked to the characteristics of the test infrastructure.

In a laboratory test setup, it is not possible to model the complete system required for a realistic TSO-DSO interaction in real hardware. Therefore, it will strongly rely on a coupling between simulated and real-world components. This section discusses the general and ICT features of the planned setup for SmartNet.

The description of the laboratory reveals the following main aspects in relation to SmartNet use cases:

- A high flexibility level is achieved to test different network and market configurations, i.e., it is valid to represent different CSs and UCs.
- Using this setup communications between different actors could be tested.
- The limit of 20 nodes seems not to be a problem considering that, in the use cases presented in previous sections (see Table 4.1), the number of system actors is eleven.
- There is a limited number of communication protocols implemented and they are linked to network asset control and monitoring. Other protocols can be introduced in the system but the effort to do so might be significant.
- The main challenges of the laboratory test environment seem to be linked to the assessment of market related communications: a market simulator should be developed (central and local markets could be based on the same principles) and the communications with that market

should be implemented to permit the observance of the procurement and activation phases presented in the previous section. The use of a SG-CG proposed standard for market interaction would be advisable (check Table 10.1).

5.4.1 General setup

AIT will employ its **LabLink Middleware** for flexible connection of dedicated simulators and real world components. LabLink is a message routing component that enables to handle simulated and real-world TCP/IP traffic between different nodes with different application protocols. A general overview of LabLink is given in the next figure.

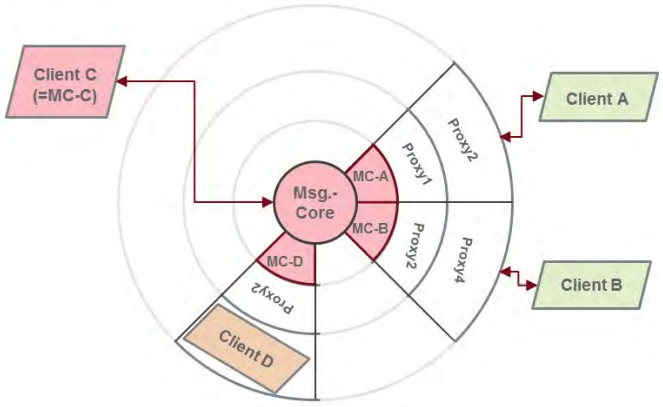


Figure 5.4 LabLink Middleware overview

The underlying idea is to realise the same message flows that would be in the real-world system in the laboratory setup. Each message flow is handled by a TCP/IP connection over the LabLink messaging core. Optional protocol conversion proxies, which can be instantiated for each LabLink node, can convert between application-level protocols used by different components. A real-world Electric Vehicle (EV) charging station talking Open Charge Point Protocol (OCPP) can, e.g., be connected to a simulated aggregator that uses proprietary simple text strings for commands towards the charging station.

Next figure depicts an example system with a market simulator, a real TSO SCADA, simulated DSO SCADA, and some flexible resources, among which one battery system is a real world battery emulator and inverter in the SmartEST lab.

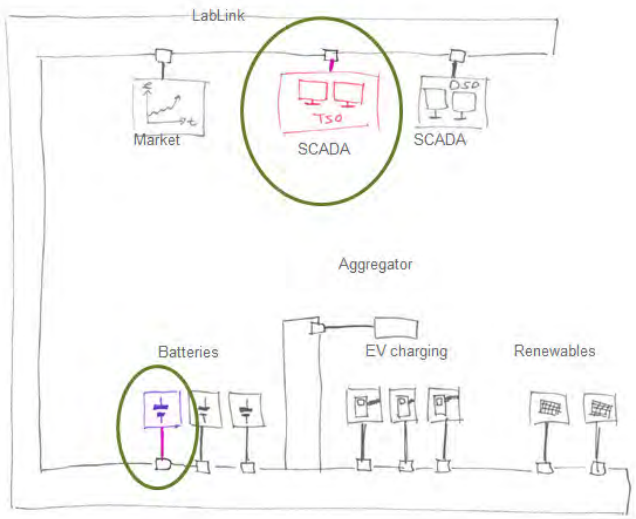


Figure 5.5 Real (colour) and simulated (grey) components connected to a LabLink instance

In this case, any communication between the TSO SCADA and the battery system, e.g. using IEC 61850, would just be routed through LabLink without any translation. However, if further resources within a power system simulator are also addressed by TSO SCADA, these messages would have to be translated in a format the simulator can work with.

The LabLink middleware does not only allow to connect simulated and real world Smart Grid components with message streams carrying different protocols, it also allows to incorporate **emulation** of the communication technologies, such as wireless or power line communications, into the setup. Figure 5.6 shows how this can be achieved.

Alternatively, a communication emulator can also be connected to two nodes of the same LabLink instances. This is up to the LabLink routing configuration. Such a system can potentially be also stripped down to its essential components and then shipped to a SmartNet project partner for testing of different emulators.

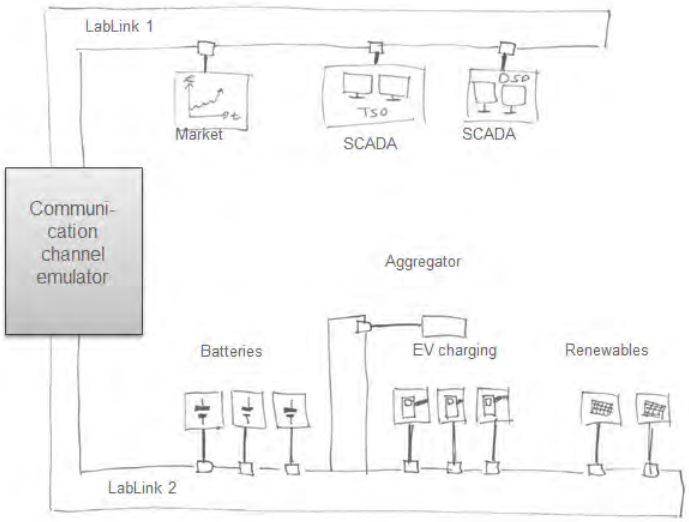


Figure 5.6 Example for a communication channel emulator connected between two LabLink instances

The use of LabLink, as a middleware connecting simulated and real-world components in the SmartNet laboratory tests, renders the test setup very flexible and allows for efficient component re-use from previous system simulations. However, a number of requirements results from the proposed setup.

5.4.2 Requirements on modelled system size

The modelled system setup is restricted in **size**. Due to performance restrictions of the approach with a central messaging core, it is not advisable to connect more than approximately **twenty nodes** to LabLink. A node can be a power system simulator, a SCADA system, a real-world lab component such as a battery system, etc.

Each node can have a number of variables that play a role in operating the setup and are accessible from LabLink. Especially if nodes are simulators, they tend to have many variables (e.g. a power system simulator with N flexible resources will have at least N variables that can be accessed via LabLink). Approximately, **200 externally visible variables** is the limit for the overall system setup.

With these restrictions in mind, the laboratory setup will most probably model a basic, conceptual system with 1-2 TSOs, 1-2 DSOs, and a few flexibilities, rather than a real world situation.

5.4.3 Requirements on Simulators for the lab test

Simulators used in the test setup have to feature a suitable interface to LabLink. The simulator must instantiate a **TCP/IP connection** to a socket provided by LabLink. Such interfaces have been made available in the past by AIT, e.g. for Digsilent PowerFactory and other simulators. Also, it is possible to add a special proxy component that interfaces with a simulator in a different fashion.

The simulators have to feature an emulation mode, where they run in **real-time**. Alternatively, they might only react on external events, and send out responses to this. This might be a suitable approach for a market simulator.

5.4.4 Requirements on real-world ICT components for the lab test

ICT components, such as aggregator management systems or SCADA systems, can be connected easily with LabLink taking into account the restriction in the number of nodes as stated above. They can have one or multiple TCP/IP connections to other components on LabLink. If no communication channel emulation is used, real-world ICT components talking to other real-world components do not necessarily have to use LabLink, but can also be connected directly. However, the use of LabLink simplifies the connection setup significantly.

5.4.5 Requirements on real-world power hardware for the lab test

The number of translations between calculated physical values (e.g. voltage, frequency, power) and physical power interfaces of real-world components is restricted by the availability of power amplifier in the SmartEST laboratory. Currently, a single 30kW, 400V, three-phase unit is available for the project. Therefore, all real-world power hardware has to be situated on a **single real-world low voltage feeder** set up in the laboratory.

Available real-world components in SmartEST are:

- Photovoltaic (PV) inverters fed by a PV module emulator.
- Charging station connected to an EV emulator.
- Battery system inverter connected to a battery emulator.

5.4.6 Requirements on communication protocols for the lab test

In principle, any application-level protocol based on TCP/IP can be used within the lab test. In many cases, however, a translation between protocols might become necessary. In that case, the communication stack of the protocol must be available. It can require significant effort to implement a translation proxy for a certain protocol, depending on its complexity. Therefore, for the lab test it would be wise to make use of protocols that are already implemented for LabLink. Currently, these are the following: IEC 60870-5-104, IEC 61850 and Modbus TCP.

6 ICT requirement prioritization

ICT requirements are captured and prioritized in top-down and bottom-up manners. In the top-down case, general smart grid requirements have been obtained from standards and recommendations. Moreover, additional requirements have been collected from coordination schemes and use cases. Each coordination scheme and use case has been analysed from the business down to the function layer. The bottom-up analysis includes the analysis of information exchange merely in communication and component layers.

The ICT requirements are classified as:

- **Smart grid requirements**: they set the general framework and reference targeting at interoperable solutions at the European level.
- **SmartNet project requirements:** they stem from the SmartNet approach defined by the coordination schemes, use cases and market design. They have also been revised in light of the technological pilot descriptions.

6.1 General smart grid framework

The following table presents examples of **general requirements** that are derived from the European smart grid approach and that can be applied to the SmartNet ICT communication and information layers.

Field	Description
Information model	A coherent and extensible information model for describing the different aspects of SmartNet must be defined to allow unambiguous exchange of information between the actors of the system. The model should be based on CIM as defined in IEC 61970-301 with extensions from other IEC standards as needed. The standards proposed at European level pursuing interoperability must be used whenever possible. For market processes, IEC 62325 is the reference (also based on CIM), while the ENTSO-E EDI provides data models. Proprietary solutions should be limited to the cases when existing standards do not suit the functionalities related to the services that need to be implemented. In some cases, end devices in process and field zones are too simple to implement complex standards and, here, the use of de-facto standards is common. This has a low impact on interoperability when the use of gateways permits to translate the information to standardized protocols "upstream" the field and station zones (see Figure 12.1).
Communication system	A communication system for reliable, efficient and secure message passing between the distributed actors of the system must be defined. The communication system should be IP-based and built on an existing message-oriented middleware standard and proven implementations.

Field	Description
Communication networks	Two main types of networks should be the most extensively used for market related communications: • Those providing connection between systems of one party (intra-control centre communications). • Those providing connections between systems of different parties (backbone networks).
Publish/subscribe	The communication system should support the publish/subscribe communication pattern to allow efficient many-to-many messaging of measurement values and similar.
Request/response	The communication system should support the request/response communication pattern to allow servers to handle requests from clients.
Quality-of-Service	The communication system must be able to document and measure Quality-of-Service (QoS) parameters such as latency, jitter, throughput, drop rates and availability within the limits of the underlying networks. Message latency in market environments is not as critical as that of other smart grid services. However, a minimum QoS should be guaranteed in communications to avoid congestions..
Gateway/interfaces	The system must provide gateways to interface with different Smart Grid standards and technologies in a seamless way. For instance, gateways should be provided to query and control DER assets. The listed core standards for Smart Grids should be supported.
Network emulation	For simulation and testing, the communication system should provide an emulation environment for IP-networks able to define network topologies and set QoS properties of links between nodes such as latency, jitter and packet drop rates.
Security	Even in market related communications are not as critical as those related to the operation of the network (limited impact on reliability), data privacy issues must be observed: integrity, availability, confidentiality, authentication and non-repudiation (see section 11). A common encoding scheme for information must be defined to facilitate information exchange among diverse systems. For CIM the defined RDF/XML mapping could be used. The use of digital certificates is also advisable. The use of private networks concentrates security risks at the interconnection points with public networks, if any.

Table 6.1 General smart grid requirements for ICTs applicable to SmartNet

6.2 SmartNet framework

The SmartNet approach defines more detailed ICT requirements in comparison to those coming from the general smart grid framework.

Coordination schemes provide detailed information about the market models, i.e. business actors and their roles, and communication links among actors. The use case specifications give detailed information about market processes and procedures, as well as about communication and computational activities that must be considered.

In the next table, a summary of ICT requirements derived from market design characteristics is presented. These requirements affect all coordination schemes and use cases.

Field	Description
Pricing	Locational nodal pricing requires a data field on node information to be included.
Bidding	The definition of bid types set the data fields that need to be included in bid messages (data models). Bids have two main parts: the bid itself plus additional optional constraint information.
Timing	The SmartNet market is discrete, cleared every 5 minutes and with a rolling optimization of one hour (this is the first assumption and parameters are subject to change during the project). These parameters set a time limit requirement for all communications and computational steps to be performed within each market session, which is normally linked to procurement and activation processes.
Clearing	The algorithm for market clearing requires some computational time to provide the expected results, basically, an economic and technical optimization of the system. This time characteristic is not known a-priori, because it depends on several factors such as the algorithm design, the hardware/software components where the algorithm is executed, the complexity of the network(s), the characteristics of the bids (e.g. optional constraints), etc. Based on the execution time of the clearing algorithm, the remaining time left for communications within each market period can be estimated.

Table 6.2 General ICT requirements from SmartNet market design

Technical ICT requirements are the outcome from the analysis of the four processes presented in the integrated use case defined in subsection 4.2. In the next Table 6.3, ICT requirements are presented for the information objects identified in the messages of the previous activity diagrams (Figure 4.5, Figure 4.6, Figure 4.7 and Figure 4.8). Before introducing the table, some general comments are presented below.

Regarding **communication requirements** the following statements can be made:

- Focusing on **procurement and activation**, which are affected by the most restrictive time limitation from market design (5 minutes under current assumption), the maximum number of messages to be delivered within each market step is 14 maximum. This number comes from counting those use case steps that require a message exchange excluding those messages that can be sent in parallel with other messages or processes (e.g. acknowledgement or reserve need/market bids/DSO constraints). The time available for communication is reduced by the time required for computation, which in these two market processes is devoted mainly to local market clearance and central market clearance including economic and technical aspects (in the use case descriptions these activities are separated while in SmartNet market design they are carried out together). From the communication's

viewpoint, the coordination schemes with local markets require a higher number of messages to be delivered and respectively a higher amount of computation.

- Only **latency** requirements referred to the performance classes defined in Table 3.1 are provided. Considering a maximum of ten seconds transfer time requirement for each message (performance class P9), which is defined as a non-critical transfer time (compared to network operation requirements), the 14 messages calculated above for the "worst case" would need around 2.5 minutes in total for message exchange. The rest would be left for computation and other possible delays, e.g. encryption involving data encoding and decoding. In five minutes step markets, half of the time would remain for other activities. Hence, estimation of the time required for computation is the key to understand. Without further inputs from simulations or system measurements, we anticipate that 2.5 minutes would be a feasible time to perform the aforementioned activities. If this is not the case, then the latency requirements need to be reduced accordingly, which in turn might limit the suitable communication technologies. Therefore, when setting requirements we need to include also performance margins to make the system more flexible for future changes. Nevertheless, for the most important messages (schedule and blocking) shorter latencies have been required and, in addition, that all of the 14 messages hit the worst-case latency of 10 seconds is a quite pessimistic assumption, because the current communication technologies have inherently smaller latencies.
- The non-critical latency requirements permit the use of most of the current **communication technologies** (see Table 3.2).
- All market interactions are foreseen to be performed through the same market platform. Therefore, **communication network types** are common for most of the links between system actors. In addition, communications will need to be bidirectional. Two main types of networks have been identified:
    - Intra data centre networks: they link systems of the same company of group of companies. Therefore, they should be probably private networks. Security and Quality of Service (QoS) performance is expected to be better than in public networks.
    - Backbone networks: since we are considering that market related communications are not critical, public networks could be used for data exchange. However, a minimum quality of service should be requested to avoid delays (congestions) and security problems.

Table 6.3 presents the data fields that should be included into the ICT requirements with respect to **information exchange**. It is advised that SG-CG proposed data standards are used whenever possible. Table 10.1, in the annex, contains examples of recommended data standards exchanged by different actors/components. Since the focus in the SmartNet project is on market related exchanges, the most

suitable standards are IEC 62325 and EDI. However, when controlling network assets and performing real-time operations over networks, standards such as IEC 61850, IEC 60870-5-104, IEC 62746, and IEC 62056 become important. More detailed information about the use of these data standards can be found in the annex section 10.

Security level requirements are defined using five criticality levels presented in Table 11.1. Although this table is intended for reliability, we have used the same levels (from low to highly critical) for data privacy issues. Regarding the security requirements, the following statements can be made:

- As mentioned before, market related exchanges do not have a direct impact on operation, and procedures are designed considering the existence of reserve, backup and emergency strategies. Therefore, in the table the top score is" High" (critical and very critical are not used).
- It is considered that **Integrity** should be high for all messages. Thus, data modifications to the exchanged data should be avoided.
- **Availability** is considered low or medium in non-time critical market processes (pre-qualification and settlement) and high in those processes inserted in market steps. Acknowledgement messages should have high availability to avoid information to be resent.
- **Confidentiality**: in general, the sensitiveness of the exchanged information is considered low. Even part of this market related information could be public, e.g. market results. Some exceptions, assigned in the table with a "High" score, are the following:
    - Network related information: constraints and measurement data.
    - Economic information: market bids and financial settlement.
- **Authentication**: it is considered high in all cases. The origin of the information must be ensured in all cases.
- **Non-repudiation**: It is considered "low" level requirement for pre-qualification and settlement processes, and "high" for procurement and activation.

In general, the security aspects are adequately and systemically planned and implemented by DSOs, TSOs, and large aggregators. The security challenges are more likely to arise from the interactions with small actors and components stationed at the edges of the grid. For example, DERs owners and small aggregators might not have sufficient competence or capital to invest on equipment and software in order to make their communication links and data secure. The architecture design itself should provide supportive means to assist and enforce small stakeholders to choose communication solutions that are sufficiently secure. Therefore, more stringent security requirements are defined for the distribution network edge information exchange.

Information object	UC phase	Communication requirements (latency)	Information requirements	Security level requirement
Pre-qualification request	Pre-qualification	P9	• Technical information of the asset: general characteristics, maximum P and Q generation/consumption capacity, typical operation values at different voltage levels • Information about the connection point of the asset: location, voltage... • Historical data of operation for baseline definition (if necessary) • General information: provider ID, request ID...	• Integrity: High • Availability: Low • Confidentiality: Low • Authentication: High • Non-repudiation: Low
Pre-qualification result	Pre-qualification	P9	• Eligible/not eligible to offer the AS • Characteristics of the service to be provided: power and/or voltage range to be provided, response time, pricing... • Operation baseline (reference to be compared against the behaviour during AS provision). If necessary • Referenced Request ID	• Integrity: High • Availability: Low • Confidentiality: Low • Authentication: High • Non-repudiation: Low
Test signal	Pre-qualification	P9	• Start and stop time • Schedule/settings to be observed during test • Test ID	• Integrity: High • Availability: Medium • Confidentiality: Low • Authentication: High • Non-repudiation: Low
Test result	Pre-qualification	P9	• Measured network parameters at grid connection node of the asset: mainly, voltage, current and power factor versus time. • General information: provider ID, test ID...	• Integrity: High • Availability: Medium • Confidentiality: Low • Authentication: High • Non-repudiation: Low

Information object	UC phase	Communication requirements (latency)	Information requirements	Security level requirement
Acknowledgement	Pre-qualification Activation (they could be present also in procurement and settlement)	P9	• Message receipt confirmation • Reference to received message: ID, receipt time. • Response time: timestamp • General information: provider ID	• Integrity: High • Availability: High • Confidentiality: Low • Authentication: High • Non-repudiation: High
Capacities update	Pre-qualification	P9	• New reactive power or droop capacities available by the service provider for each of the indicated market periods (Q-time or droop time curves): magnitude, market step (date, no. of session, starting and ending time of the step)... • General information: provider ID	• Integrity: High • Availability: High • Confidentiality: Low • Authentication: High • Non-repudiation: High
Reserve needs	**Procurement**	P9	• Active power quantity required for each period of the market: magnitude, market step • Buyer ID	• Integrity: High • Availability: High • Confidentiality: Low • Authentication: High • Non-repudiation: High
Network constraints	**Procurement**	P9	• Grid operator ID • Power limit linked to each node (node ID) • Market session step	• Integrity: High • Availability: High • Confidentiality: High • Authentication: High • Non-repudiation: High
DER flexibility	**Procurement**	P9	• DER owner ID, node ID, Aggregator ID, AS ID • P or Q reduction/increase available vs. time or market period • Price	• Integrity: High • Availability: High • Confidentiality: High • Authentication: High • Non-repudiation: High

Information object	UC phase	Communication requirements (latency)	Information requirements	Security level requirement
Market bid	**Procurement**	P9	• SmartNet marked bid formats have been referenced in subsection 4.3 above. Please, check for details. • Other aspects to be considered: market ID, AS ID, market session ID	• Integrity: High • Availability: High • Confidentiality: High • Authentication: High • Non-repudiation: High
Market results	**Procurement**	P9	• List of accepted bids (bid ID), for each market step (market session reference) • Bid characteristics: provider ID, node ID, active power for each market step, offered price • General information: market operator ID, market session ID, locational marginal prices information, timestamp, etc.	• Integrity: High • Availability: High • Confidentiality: Low • Authentication: High • Non-repudiation: High
Blocking	**Activation**	P4	• DSO ID • Bid to be blocked (bid ID) • Affected distribution Node ID • Cause of the blocking (e.g. voltage limit violation) • Market step reference • Timestamp	• Integrity: High • Availability: High • Confidentiality: High • Authentication: High • Non-repudiation: High
Schedule/Setting (activation)	**Activation**	P4	• Schedule message has the same format as the market result message above. • Setting message must indicate at least: magnitude (reactive power, voltage, power factor, droop), provider ID, node ID and market step.	• Integrity: High • Availability: High • Confidentiality: Low • Authentication: High • Non-repudiation: High

Information object	UC phase	Communication requirements (latency)	Information requirements	Security level requirement
Measurement	Settlement	P9	• Measurement of network parameters versus time: voltage, current, active power, reactive power, measurement time... • General information: provider ID, node ID, asset ID	• Integrity: High • Availability: Low • Confidentiality: High • Authentication: High • Non-repudiation: Low
Financial settlement	Settlement	P9	• General information: bid reference, provider reference • Commitments acquired in the bid: magnitude, market step • Measurement of network parameters: same as for Measurement message. • Economic information: service payment (it could have different terms: fixed, variable, independent of/tight to activation...), taxes, etc. • Payment details: bank information, due date, etc.	• Integrity: High • Availability: Low • Confidentiality: High • Authentication: High • Non-repudiation: Low

Table 6.3 ICT requirements from SmartNet use cases (from business and function layers)

The last iteration of the ICT requirement analysis is done in a bottom-up manner by analysing information exchange activities for each communication link at the communications and component levels. The requirements were collected from each use case (out of the previous 7), which are currently being harmonised in two ways. The use case specific ICT requirements are aggregated and generalised according to pre-qualification, procurement, activation and settlement procedures. The requirements associated with information exchanges are aggregated using more generic requirement classes for networking, security, latency, data size/data rate, cost, and protocols. The final requirements in the requirement table are presented in a unified format keeping the links to the original use case descriptions. An example of the ICT requirement table is shown in Table 6.4.

Use Case Information Exchanged	System actors	Information Object	Description	Requirement Class
UC2_A(IEX_01)	CMP EMS -> DSO EMS	*IE_Prequalification*	Request prequalification assessment	*RC_Prequalification*
UC2_A(IEX_02)	CMP EMS -> DSO EMS	*IE_PrequalificationResult*	Send prequalification results	*RC_Prequalification*
UC2_A(IEX_03) UC2_C(IEX_03)	AS market platform (CMP) -> AS market platform (TSO)	*IE_MarketBids*	Market bids consist of a capacity (€/MW) and energy component (€/MWh)	*RC_CMPtoMarket*

Networking properties	Security	Latency	Data size/ Data rate	Cost	Protocol Class
Two ways communication P2P Availability Multi technology support	Authorization / Authentication: 3 Integrity: 3	Type 5	150 - 1000 Bytes / 9.6 kbps	Medium	*PC_EnergyMarket*
Two ways communication P2P Availability Multi technology support	Authorization / Authentication: 3 Integrity: 3	Type 5	150 - 1000 Bytes / 9.6 kbps	Medium	*PC_EnergyMarket*
One way communication P2P Availability Reliability and security	Authorization / Authentication: 3 Integrity: 3 Confidentiality: 2	Type 5	150 - 1000 Bytes / 9.6 kbps	Medium	*PC_EnergyMarket*

Table 6.4 ICT requirements from SmartNet use cases (communications and component layers).

The data aggregation enables us to reduce the number of ICT requirements into manageable size and makes them more comprehensive for the forthcoming architecture design work. Moreover, this unified requirement table gives us a tool to compare ICT requirements affecting different coordination schemes and use cases. It also provides a tool to make prioritisation and thus to concentrate on requirements that are vital for the communication architecture design as well as for the technology pilots and simulation environment.

The prioritisation work continues during the architecture design phase. The table will also be refined and updated according to additional information obtained from other project tasks, and state-of-the-art surveys focusing on existing and forthcoming energy and communication architectures. The final prioritisation table will be presented in D3.2 Architecture design report.

7 Conclusions

The deliverable summarises the ICT requirements derived from the SmartNet project approach based on the coordination schemes, use cases and market characteristics. These requirements are set in the context of the standards and methodologies promoted at EU level to achieve interoperable solutions for smart grids. The deliverable is the core element for elaborating the ICT architecture design to support proposed market models and coordination schemes.

The focus of the ICT is set on the AS market related interactions between actors, however a broader perspective is provided in the document to cover other relevant smart grid zones and domain communications, e.g., control and monitoring of flexible resources.

The following aspects can be highlighted with regard to **general ICT requirements** from the analysis performed in the previous sections:

- The main ICT requirements have been identified are summarized in chapter 6. They are classified as:
  - **General smart grid framework**: derived from the European smart grid approach (Table 6.1).
  - **SmartNet project framework**: market design (pricing, bidding, timing and clearing) related requirements (Table 6.2); and main requirements for information exchange in AS market processes, including data types to be transmitted, latency, security and types of networks (Table 6.3 and Table 6.4).
- Market processes are considered **non-critical**, with maximum allowed transfer times of 10 seconds. The non-critical latency requirement makes most of current communication technologies suitable to meet market interaction needs. As smart grids deployment grows, lower latencies are likely to be required for message exchange. In similar way, communication technologies are evolving towards faster, more flexible, and more reliable solutions (5G / IoT).
- The **security requirements** need to be more stringent at the edges of the grid. Small stakeholders may not have sufficient competence or capital to invest on equipment and software in order to make their communication links and data secure. As a result, the architecture design itself should provide supportive means to assist and enforce small stakeholders to choose communication solutions that are sufficiently secure.
- **Pre-qualification** and **settlement** are the less-time critical market processes from the ICT point of view, since they are normally detached from the intra-day operation of the network. By contrast, all procurement and activation processes should fit within each market step window.

- A general requirement is that all market related communications, from bids to settings and blocking signals, is performed through the **market operator platform**. This standardizes and provides uniformity to the communications.
- In market schemes, the **activation** of flexibility assets is performed by their own operators as result of the economic market clearance and subsequent technical constraint resolution process. Therefore, no specific activation signal is required but a communication of the schedules and settings for the next market periods.
- The **standards proposed at European level** pursuing interoperability must be used whenever possible. For market processes, IEC 62325 is the reference (based on CIM), while the ENTSO-E EDI provides data models and is related to the previous. Proprietary solutions should be limited to the cases when existing standards do not suit the functionalities related to the services that need to be implemented. In some cases, end devices in process and field zones are too simple to implement complex standards and, here, the use of de-facto standards is common. This has a low impact on interoperability when the use of gateways permits to translate the information to standardized protocols in the field and station zones.
- Two **communication network types** are expected to be used for most of the interactions with the market: intra-data centre network and backbone networks.

Regarding **coordination schemes** and **use cases**, attention should be paid to the following points affecting ICTs:

- Those CSs with **local market** structures (B, C, D2) have additional steps related to local market processes and this involves a higher number of message exchange and computation periods. However, it is difficult to conclude from this that they require longer times to carry out all processes, this will be linked to the computation times required under each scheme.
- In the use case description, it is considered that **market clearance** and **technical constraints resolution** are performed by different business actors. However, the SmartNet algorithm considers both processes and, therefore, they are performed only by the market operator. From the ICTs perspective, on the one side, this reduces the number of messages between system and market operator but, on the other side, it involves challenges in terms of, e.g., data confidentiality, responsibility of network operation and transmission of network sensitive information. This affects mainly CS E.
- CS A - variant 2, where the **TSO monitors the distribution network**, seems to be challenging from ICT perspective: the setting up of the infrastructure and/or the definition of data exchanges between DSO and TSO. A completely new set of rules, including ICT requirements, would have to be defined to permit such a monitoring and control approach.

- **Variant D1**: it is to be established how the joint market operation between DSO and TSO impact on ICTs: which party will undertake market operator role (e.g. a new company belonging to both actors)? And what types of information exchange needs will arise?

With respect to **market design** the following must be considered:

- The **maximum available time for message exchange** is the market clearance window (e.g. 5 minutes), minus the time required for computation. This available time sets maximum latency requirements for messages. It should be considered that some messages can be sent in parallel, while others require series processing and involve longer time for communications. Possible delays related to the quality of service should be also taken into account to identify the maximum available time for message exchange. Computation time requirements are difficult to know a-priori because they depend on the algorithm, the hardware where it is installed, the simulated network complexity, the types of bids involved, etc. Therefore, safety margins are needed for the communications.
- Several **data models** have been identified in existing standards. It can be concluded that data models related to, e.g., bids, market results, acknowledgement and settlement, already exist in IEC 62325. A further assessment should be performed to check how well these data models fit into the SmartNet design, e.g., the three types of bids defined in the market and the use of optional information.
- From the bid design in the SmartNet market, it is not defined whether the so called **optional information** should be integrated or not in the main bid message. In principle, including all the information in the same message should be more efficient than sending two separate messages.

Pilots and the **laboratory setup**, together with simulations, are devoted to test the feasibility of the SmartNet approach defined by CSs, UCs and market features. The pilots offer a good opportunity to test innovative ICT approaches that are expected to become relevant in the future, as IoT related solutions. However, the following ICT related aspects should be considered:

- **Pilot definitions** are focused on network monitoring and control activities more than on market related communications. Even if pilots are referred to CSs and UCs, it is not clear how the TSO-DSO relationship schemes will be realized and how distributed network DERs are integrated in market frameworks.
- Pilot A approach seems to be linked to current schemes, which could be defined as a mix of CS A and CS C, meaning centralized market control by the TSO but no local market involvement.
- In pilot B, the duration of control and measurement loop is designed to last for 5 minutes, which may significantly affect the service provision due to the limited visibility of flexibility assets.

- The **laboratory setup** used in SmartNet presents high flexibility and permits to test different network and market configurations whether they are valid for different CSs and UCs. However, this flexibility is restricted by the characteristics of the test infrastructure. The main challenges seem to be linked to market related communications. For this, the market simulator should be developed (central and local markets could be based on the same principles) and the communications with that market should be implemented. This may require a significant amount of effort.

8 References

[1] "Basic schemes for TSO-DSO coordination and ancillary services provision", SmartNet project deliverable D1.3, draft version, 14/10/2016

[2] "Market design for centralised coordination mechanisms", SmartNet project deliverable D2.4, draft version, 15/09/2016

[3] "Smart Grid Reference Architecture", CEN-CENELEC-ETSI Smart Grid Coordination Group, 11/2012 [available online: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Reference_Architecture_final.pdf]

[4] "SGCG/M490/K_SGAM usage and examples, SGAM user manual - Applying, testing & refining the Smart Grid Architecture Model (SGAM) Version 3.0", CEN-CENELEC-ETSI Smart Grid Coordination Group, 11/2014 [available online: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Methodology_SGAMUserManual.pdf]

[5] "SGCG/M490/G_Smart Grid Set of Standards Version 3.1", CEN-CENELEC-ETSI Smart Grid Coordination Group, 31/10/2014 [available online: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Standards_Report.pdf]

[6] "IEC 61850-5 Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models", IEC International Standard, TC 57, edition 2.0, 01/2013

[7] M. Elneel, "Theory & practice of ICST adoption within the smart grid ecosystem", McMaster University, September 15, 2014 [available: http://wbooth.mcmaster.ca/epp/publications/student/2014/MElneel.pdf]

[8] M. Kuzlu, M. Pipattanasomporn, "Assessment of communication technologies and network requirements for different smart grid applications, Innovative Smart Grid Technologies (ISGT)", IEEE PES, 02/2013

[9] M Uslar, M Specht, S Rohjans, J Trefke, JM González, "The Common Information Model CIM: IEC 61968/61970 and 62325-A practical introduction to the CIM", 2012

[10] Teach-ICT.com, [online: http://www.teach-ict.com/gcse_computing/ocr/211_hardware_software/reliability/miniweb/index.htm, last accessed: 06/2016]

[11] C. Caerts, C. Tornelli, L. Radaelli, E. Rikos, M. Uslar, ·"Description of the methodology for the detailed functional specification of the ELECTRA solutions", , EU FP7-ENERGY-2013 programme, ELECTRA project no. 609687, Deliverable R4.1, 16/01/2015

[12] ""LTE for smart grid communication - the Canadian outlook", IEEE Canadian Review, Spring 2014 [available: http://canrev.ieee.ca/cr72/index.htm, accessed: 05/2016]

[13] Güngür, V. C., Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., & Hancke, G. P., "Smart grid technologies: Communication technologies and standards". IEEE Transactions on Industrial Informatics, 7(4), 529–539. 2011 [available: http://doi.org/10.1109/TII.2011.2166794]

[14] Mulla, A., Baviskar, J., Khare, S., & Kazi, F. "The Wireless Technologies for Smart Grid Communication: A Review", 2015 Fifth International Conference on Communication Systems and Network Technologies, 442–447, 2015 [available: http://doi.org/10.1109/CSNT.2015.146]

[15] "3GPP" [online: http://www.3gpp.org/, last accessed: 05/2016]

[16] K. Mallinson "The path to 5G: as much evolution as revolution", 3GPP, 10/05/2016 [online: http://www.3gpp.org/news-events/3gpp-news/1774-5g_wiseharbour, last accessed: 05/2016]

[17] A. Castonguay, E. Buckland, M. Hatton "2G and 3G switch-off: a navigation guide for IoT", Machina research, 02/11/2015 [available: https://machinaresearch.com/report/2g-and-3g-switch-off-a-navigation-guide-for-iot/]

[18] "Internet of Things (IoT)", IoT Agenda, Techtarget [online: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT, last accessed: 06/2016]

[19] "LTE-evolution for IoT connectivity", Whitepaper, Nokia, 2016 [available: http://resources.alcatel-lucent.com/asset/200178]

[20] "XBee products", DIGI [online: http://www.digi.com/products/xbee, last accessed: 05/2016]

[21] Dash7 Alliance, [online: http://www.dash7-alliance.org/, last accessed: 05/2016]

[22] M. Weyn et al., "Survey of the DASH7 Alliance protocol for 433 MHz Wireless sensor communication", International journal of distributed sensor networks, Volume 2013, Article IC 870430, 2013 [available: http://95.85.41.106/wp-content/uploads/2014/08/hindawi-oss.pdf]

[23] Sigfox, [online: http://www.sigfox.com/, last accessed: 05/2016]

[24] LoRa Alliance, [online: https://www.lora-alliance.org/, last accessed: 05/2016]

[25] "SigFox Vs. LoRa: a comparison between technologies & business models", LinkLabs, 13/01/2016 [online: http://www.link-labs.com/sigfox-vs-lora/, last accessed: 05/2016]

[26] "LoRa vs. LTE-M vs. Sigfox", Creative Connectivity, 22/12/2015, [online: http://www.nickhunn.com/lora-vs-lte-m-vs-sigfox/, last accessed: 05/2016]

[27] B. Moyer, "Low power, wide area - A survey of longer-range IoT wireless protocols", 07/09/2015, [online: http://www.eejournal.com/archives/articles/20150907-lpwa/, last accessed: 05/2016]

[28] "Energy Interoperation version 1.0 (specification)", OASIS Standard, 11 June 2014 [available online: http://docs.oasis-open.org/energyinterop/ei/v1.0/os/energyinterop-v1.0-os.html, last accessed: 29/04/2016]

[29] "ENTSO-E EDI Work Products Library", ENTSOE [online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/Pages/default.aspx, last accessed: 20/04/2016]

[30] "The harmonised electricity market role model", ENTSO-E, 2015-01 [available online: https://www.entsoe.eu/Documents/EDI/Library/HRM/5_Harmonised-role-model-2015-01-for-approval-2015-09-30.pdf, last accessed: 20/04/2016]

[31] "MADES communication standard", ENTSO-E, version 1.1, 20/06/2014 [available: https://www.entsoe.eu/fileadmin/user_upload/edi/library/mades/mades-v1r1.pdf]

[32] "ETSO Modelling Methodology for the Automation of Data Interchange of Business Processes (EMM)", ENTSO-E [available online: https://www.entsoe.eu/fileadmin/user_upload/edi/library/emm/emm-v1r4.pdf, last accessed: 20/04/2016]

[33] "ENTSO-E Capacity Allocation and Nomination (ECAN)", ENTSO-E [available online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/ECAN/Pages/default.aspx, last accessed: 20/04/2016]

[34] "ENTSO-E Scheduling System (ESS)", ENTSO-E [available online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/ESS/Pages/default.aspx, last accessed: 20/04/2016]

[35] "ENTSO-E Reserve Resource Process (ERRP)", ENTSO-E [available online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/ERRP/Pages/default.aspx, last accessed: 20/04/2016]

[36] "ENTSO-E Settlement Process (ESP)", ENTSO-E [available online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/ESP/Pages/default.aspx, last accessed: 20/04/2016]

[37] "ENTSO-E HVDC Link Process", ENTSO-E [available online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/HVDC-Link-Process/Pages/default.aspx, last accessed: 20/04/2016]

[38] "Critical Network Element Implementation", ENTSO-E [available online: https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/critical-network-element-implementation/Pages/default.aspx, last accessed: 20/04/2016]

[39] "IEC 60870-5 Telecontrol equipment and systems - Part 5: Transmission protocols - All parts", IEC International Standard, edition 1.0, 2016

[40] "IEC 60870-6-503 Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 Services and protocol", IEC International Standard, edition 3.0, ISBN: 978-2-8322-1647-7, 07/2014

[41] "IEC 61850-7-420 Communication networks and systems for power utility automation – Part 7-420: Basic communication structure – Distributed energy resources logical nodes", IEC International Standard, edition 1.0, March 2009

[42] J. Schmutzler, C.A. Andersen, C. Wietfeld, "Evaluation of OCPP and IEC 61850 for Smart Charging Electric Vehicles", EVS27 conference paper, Barcelona, November 2013

[43] A.B. Pedersen, E.B. Hauksoon, P.B. Adersen, B. Poulsen, C. Træholt, D. Gantenbein, "Facilitating a generic communication interface to distributed energy resources", IEEE, First IEEE conference on Smart Grid communications, October 2010

[44] "IEC 61850-90-8 TR Communication networks and systems for power utility automation - Part 90-8: Object model for E-mobility", IEC International Standard, edition 1.0, 2016

[45] "IEC 61968-1 Application integration at electric utilities - System interfaces for distribution management - Part 1: Interface architecture and general recommendations", IEC International Standard, edition 2.0, ISBN: 978-2-83220-425-2, 10/2012

[46] "The DLMS communication survival Kit", icube software, web site [online: http://icube.ch/DLMSSurvivalKit/dsk1.html, last accessed: 05/2016]

[47] R. Schmidt, A. Caldevilla, A. Kovács et al., "V2G Interface specifications between the electric vehicle, the local smart meter, and ITS service providers", PowerUp EU project FP7 INFSO-ICT 285285, Deliverable 4.1, 04/07/2012 [available: http://www.power-up.org/wp-content/uploads/2012/07/PowerUp_D4.1_final.pdf]

[48] "Common Information Model (CIM) for Energy Markets", ENTSO-E, [online: https://www.entsoe.eu/major-projects/common-information-model-cim/cim-for-energy-markets/Pages/default.aspx, last accessed: April 2016]

[49] "IEC 62325-301 Framework for energy market communications - Part 301: Common information model (CIM) extensions for markets", IEC International Standard, edition 1.0, 05/2014

[50] "IEC 62325-351 Framework for energy market communications - Part 351: CIM European market model exchange profile ", IEC International Standard, edition 1.0, 09/2013

[51] "IEC 62325-451-1 Framework for energy market communications - Part 451-1: Acknowledgement business process and contextual model for CIM European market", IEC International Standard, edition 1.0, 10/2013

[52] "IEC 62325-451-2 Framework for energy market communications - Part 451-2: Scheduling business process and contextual model for CIM European market", IEC International Standard, edition 1.0, 05/2014

[53] "IEC 62325-451-3 Framework for energy market communications – Part 451-3: Transmission capacity allocation business process (explicit or implicit auction) and contextual model for European market". IEC International Standard, edition 1.0, 07/2014

[54] "IEC 62325-451-4 Framework for energy market communications – Part 451-4: Settlement and reconciliation business process, contextual and assembly models for European market", IEC International Standard, edition 1.0, 11/2014

[55] "IEC 62325-451-5 Framework for energy market communications - Part 451-5: Problem statement and status request business processes, contextual and assembly models for European market", IEC International Standard, edition 1.0, 02/2015

[56] "IEC TS 62325-503 Framework for energy market communications – Part 503: Market data exchanges guidelines for the IEC 62325-351 profile", IEC Technical Specification, edition 1.0, 01/2014

[57] "IEC TS 62325-504 Framework for energy market communications – Part 504: Utilization of web services for electronic data interchanges on the European energy market for electricity", IEC Technical Specification, edition 1.0, 05/2015

[58] "OpenADR 2.0 Profile Specification, B Profile", Updated 07-01-2013, Revision Number: 1.0, Document Number: 20120912-1, [available online: http://www.openadr.org/, last accessed: 04/2016]

[59] "IEC PAS 62746-10-1 Systems interface between customer energy management system and the power management system - Part 10-1: Open Automated Demand Response (OpenADR 2.0b Profile Specification)", IEC [online: https://webstore.iec.ch/publication/7570, last accessed: 05/2016]

[60] "Universal Smart Energy Framework", web site [online: http://www.usef.energy/, last accessed: 05/2016]

[61] M. Kost, "Wireless ecosystems for smart energy and home automation", Cambridge wireless, Conference: Advances in short-range wireless for mass-market applications, 30/05/2012 [available online: http://www.cambridgewireless.co.uk/crmapp/EventResource.aspx?objid=39577]

[62] "ZigBee Smart Energy", ZigBee Alliance, web site [online: http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbeesmartenergy/, last accessed: 05/2016]

[63] Rumen Kyusakov, Jens Eliasson, Jan van Deventer and Jerker Delsing, Robert Cragie, "Emerging Energy Management Standards and Technologies - Challenges and Application Prospects", IEEE, Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012), E_ISBN: 978-1-4673-4736-5, 09/2012

[64] "EEBUS", web site [online: https://www.eebus.org/, last accessed: 05/2016]

[65] "CSEP - Consortium for SEP 2.0 interoperability", web site [online: http://www.csep.org/, last accessed: 05/2016]

[66] "Smart grid security: Annex II. Security aspects of the smart grid", ENISA, 25/04/2012, [available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations]

[67] "SGCG/M490/H_Smart Grid Information Security", CEN-CENELEC-ETSI smart grid coordination group, Intermediate report v.1, December 2014 [available: http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx]

[68] L. Langer, P. Smith, M. Hutle, "Smart Grid Cybersecurity Risk Assessment Experiences with the SGIS Toolbox", 2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST), 475–482, 2015 [available: http://doi.org/10.1109/SEDST.2015.7315255]

[69] M. Hutle, G. Hansch, W. Fitzgerald, "SPARK D2.2 Threat and Risk Assessment Methodology", 2015 [available: https://project-sparks.eu//wp-content/uploads/2014/04/D2_2_Threat_and_Risk_Assessment_Methodology.pdf]

[70] "Reliability considerations from the integration of smart grid", NERC, December 2010 [available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGTF_Report_Final.pdf]

[71] "IEC 62351-3 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP", IEC International Standard, TC57 WG15, 10/2014

[72] "IEC TC 57 WG15 Public site", UCA international users group, IEC TC 57 [online: http://iectc57.ucaiug.org/wg15public/default.aspx, last accessed: 07/2016]

[73] F. Cleveland, "IEC TC57 WG15 – Data and Communication Security Status & Roadmap ", IEC TC 57 WG15 Status of 62351 presentation, 03/2016 [available: http://iectc57.ucaiug.org/wg15public/default.aspx]

9 Appendix A: Communication technologies in smart grids

In the smart grid context, different types of communication networks can be identified. These networks are used to provide services at different network zones and domains (in accordance to SGAM definitions), through the most suitable communication technologies for that purpose. This has already been considered, from a comprehensive point of view, by the SG-CG for general smart grid use cases. The following networks are identified in [5] for the smart grid environment:

A. **Subscriber Access Network**: they provide general broadband access (e.g. internet) for customer premises (home, industry, commerce). They are normally provided by communication service providers.
B. **Neighbourhood Network**: networks between distribution substations and end users. They are purpose built networks, which may service metering, distribution automation and EV charge, for example.
C. **Multi-services backhaul network**: at distribution level upper tier. They link "lower" networks (e.g. neighbourhood) with control centres or primary substations to facilitate substation level distributed intelligence (e.g. advanced metering or distribution automation services).
D. **Low-end intra-substation network**: networks inside secondary substations. They usually connect RTUs, circuit breakers and sensors.
E. **Intra-substation network**: networks inside a primary substation. They are involved in low latency critical functions such as tele-protection. They may comprise from one to three buses (system bus, process bus, and multi-services bus).
F. **Inter-substation network**: networks connecting substations between them and with control centres. The WANs have strict end performance requirements with regards to latency. They require flexible scalability and, likely, also mixed physical media and multiple aggregation topologies. System control tier networks provide networking for SCADA, for example, as well as peer-to-peer connectivity for tele-protection and substation level distributed intelligence.
G. **Intra-control centre / intra-data centre network**: they provide connectivity for systems inside the facility and connections to external networks. Both networks are at the same logical tier level but control centres connect to real time systems with high levels of security.
H. **Backbone network**: inter-enterprise network, including backbone internet, as well as inter-control centre networks.
L. **Operation Backhaul network**: they usually inter-connect network devices or subsystems (station level) to the operation level over a WAN.
M. **Industrial Fieldbus area network**: they interconnect process control equipment, mainly in power generation (bulk and DER) in the scope of smart grids.

N. **Home and building integration bus network**: they interconnect home/building communicating components and subsystems.

Normally, the fulfilment of services involves more than one type of network. For example, metering, which is based on AMI, may rely on networks B (from end-users to primary substations), C (from primary substations to HES) and G (for the exchange of information between utility backend systems); distribution automation may rely on networks L and D; demand response strategies on A and N; etc.

The communication technologies most commonly used (in bold) and/or suitable for each network type [5] are mapped to the SGAM framework in the figure below. Several options exist for each zone and domain, and the final architecture deployed should be assessed case per case based on the service to be provided, availability, cost, etc.

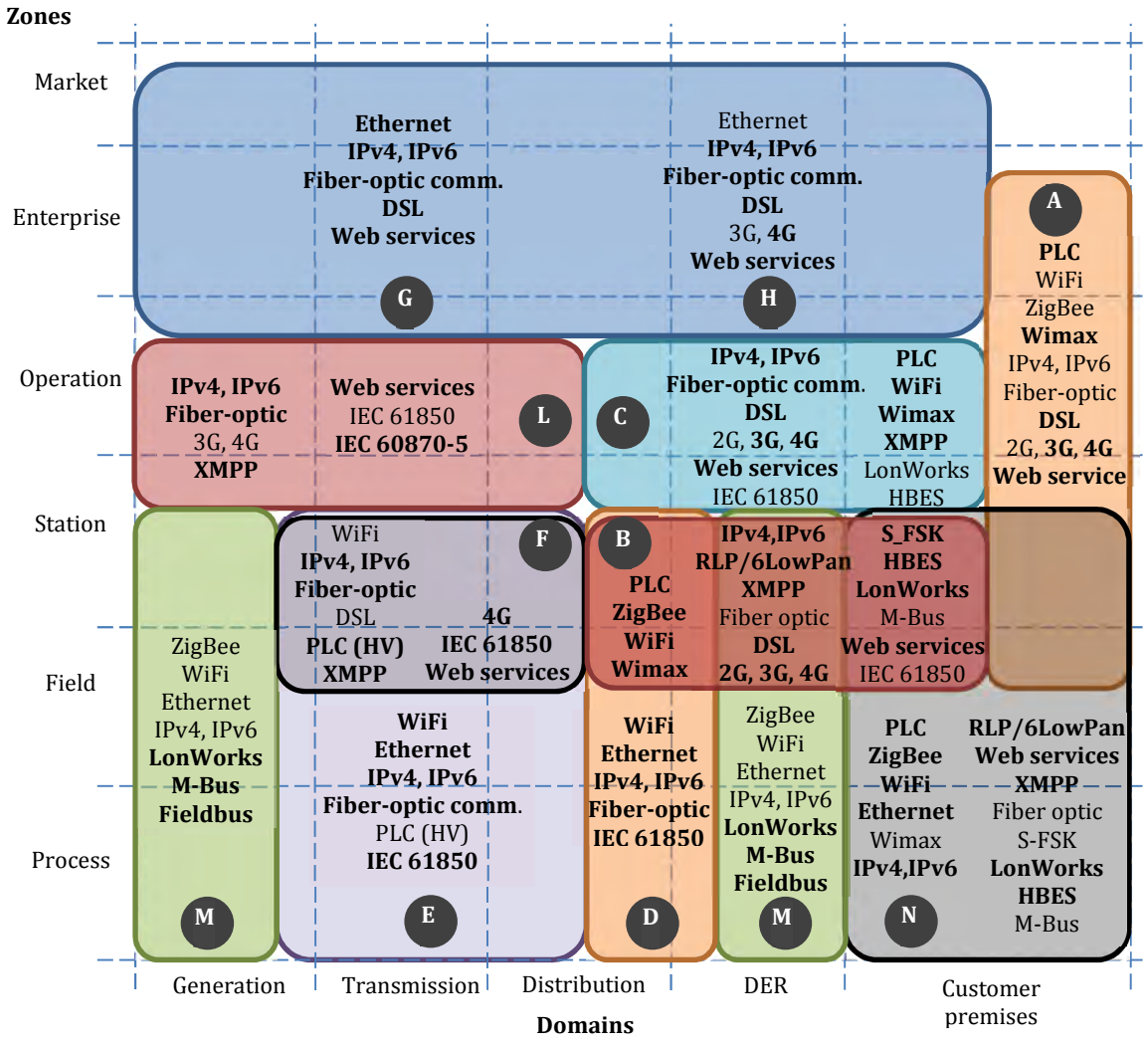


Figure 9.1 Overview of smart grid communication technologies mapped to SGAM

The technologies in the figure above are those proposed by the SG-CG pursuing interoperability throughout Europe in accordance to international standards. However, some protocols became de-facto standards and their use is wide in their fields of application, e.g. Modbus for connecting electronic devices between the process and station zones. Other technologies are currently under development but may become widely deployed in the future and proposed as reference, e.g. 5G, some low power wireless technologies related to the Internet of Things (IoT), etc.

In order to select a communication architecture some of the following **features** should be considered ([7] and others):

- Scalability
- Access layer density
- Interface flexibility (connectivity to the system using network switch ports)
- Bandwidth
- Latency
- Open-standards support
- Coverage (distance, mobile of fixed stations, etc.)
- Data routing methods: point to point (unicast, anycast) or point to multipoint (broadcast, multicast, geocast)
- Data flow direction: simplex, half-duplex, full-duplex, full-duplex emulation
- Subnetwork hierarchy
- Cost
- Ownership
- Wireless communication efficiency: available spectrum, spectral efficiency and frequency re-use
- Availability
- Reliability and security (including data protection)

Most of the characteristics above are directly related to the service to be provided, which involves specific characteristics of information exchange (see next section). In many cases, there is not one single option fitting all requirements and, therefore, a combination of technologies is used. Another reason for this is the need for redundancy.

One of the important choices related to the communication system design is the **ownership** of the infrastructure. Three models are possible:

- **Private**: the network is deployed by a private party for its own use. It allows full control and access, which results in high QoS level. In WAN, the infrastructure involves high costs for both installation and spectrum acquisition, if required. It may lead to network underutilization. Private network owners in the smart grid context are normally, on the one hand, utilities,

which seek to fulfil the functionalities and services linked to their business and roles, such as AMI and distribution automation; and, on the other, aggregators, building owners, etc.

- **Public**: operators with **licensed spectrums** for certain frequency range (e.g. cellular networks) offer telecom services. Problems might be a higher congestion of networks and higher security risks. However, today, most operators are able to offer Service Level Agreements (SLA), meeting more demanding requirements from clients. **Unlicensed spectrums** are also available for many technologies. They are free but subject to much unpredictable interference situations: QoS and availability cannot be guaranteed. Combining licensed and unlicensed spectrum is possible when both critical and less demanding functionalities are required.
- **Mix of public and private**: their main benefit is redundancy. Two examples of this type of networks are presented in [12]: a private virtual network operator with no license or infrastructure but with own SIM range, billing system, etc.; and a semi-private LTE network shared with public safety (which is being implemented in the USA).

As introduced in Figure 9.1, different communication standards exist for wired and wireless networks. For LANs internal to an enterprise or a control centre, Ethernet standards (IEEE 802.3) are ubiquitous, and provide high-speed communication at low cost. For wireless LAN, Wi-Fi standards (IEEE 802.11 family) and others are widespread.

The technologies providing lowest **latency** times (fastest communications) are fiber optic communications, Ethernet and high performance microwave, which are suited for network protection functionalities (response below 10ms). When responses around 20ms are requested, LTE-Advanced technologies are also eligible and around 100ms, the WiMAX technology could also be an option. Above 500ms, most communications would be suitable, including 3G, PLC and Radio-Frequency mesh communications [7]. However, latency is normally related to the physical layer. In wireless systems, the latency fluctuation is an inherent challenge. Moreover, the data transmission frequency affects the latency, since modern wireless systems tend to release radio resources if the communication link is not active enough. Additional delays in the transmission may exist and should be considered within the transfer time due to, for example, time required to establish a Virtual Private Network (VPN) tunnel for secure communications, congestions in public networks, etc.

Some relevant WAN communication standards and technologies are presented in the table below [13][14]:

Technology	Description
DSL	Digital subscriber line over wired phone networks. Capable of high speed up to at least 100 Mb/s, depending on the technology and the quality
GPRS (2.5G)	Wireless data over cellular GSM networks. Capable of up to 115,2 Kb/s with range 0,5-35 km.
UMTS (3G)	Wireless data over cellular networks. Capable of up to 115,2 kb/s with range 0,5-35km.
WiMAX (4G*)	Wireless last mile broadband access (IEEE 802.16). Capable of up to 37 Mb/s with range 10-50 km.
LTE (4G*)	Wireless data over cellular networks. Capable of up to 100 Mb/s. Actual speed results do not match the limits reached at test labs.
LTE-A (4/4.5G/4G+)	Wireless data over cellular networks. Capable of up to 300 Mb/s. Actual speed results will not match the maximal reached at test labs.

(*) Neither WiMAX nor LTE are truly 4G, as they do not meet the ITU demands.

Table 9.1 WAN communication standards

In the next subsections, two groups of communication technologies are presented more in detail, due to their current and future expected importance: mobile networks and Internet of Things (IoT) technologies.

9.1 Telecom network functionalities

Wide Area Network (WAN) communication is a key element to build a smart grid. A reliable communication infrastructure has to ensure that information can be exchanged everywhere under required Service Level Agreements (SLA) in a secure manner.

Today, communication is merely based on Internet Protocol (IP) and allows the use of standardised components and functionalities. This is the basis for a standardised interworking between systems. Market specific solutions will be built on top of the IP layer.

Telecom networks provide functionalities in different areas to ensure features such as:

- Coverage
- Reliable connectivity
- Data security and privacy
- Interworking with customer infrastructure
- Automated and cost efficient processes to manage connections

The telecom network provides end-to-end transport functionalities. In most cases, the communication is established between geographically distributed devices on one side and central servers on the other. In most deployments, a Multiprotocol Label Switching (MPLS) core is connecting all the different sides. The

MPLS core together with connected gateways ensures that, independently of the selected access type, an exchange between all connected sides is possible.

Coverage will be provided by hybrid solutions. Each of the selected access technology has its relevance and purpose. In many cases, a combination of access technologies will be used to fulfil specific requirements in a cost effective way.

The underlying access technology is, in most cases, provided by **Public Land Mobile Networks** (PLMN), e.g. 2G, 3G or LTE networks. These are able to offer nationwide coverage in high quality. Roaming between different PLMNs is possible and increases the coverage and the reliability, due to deep standardisation efforts carried out by the 3GPP [15] body in the last years.

Current LTE technology builds upon 3GPP releases 8 to 14 (already completed). Future releases 15 and 16 will define the LTE-Advanced Pro technology (4.5G or pre-5G), and 5G phase 1 deployments are expected for year 2020 [16].

For coming developments or upgrades of smart grids, the selected WAN technology should be LTE or further evolutions. LTE represented a significant upgrade in terms of throughput when compared, for example, to one of its closest predecessors, HSPA, by providing a theoretical throughput with three to four performance increase in the downlink (up to 300 Mbps) and two to three times levels in the uplink (up to 75 Mbps). Nowadays, LTE is highly praised and considered the most advanced telecommunications technology currently available and the only one that defines a clear path toward future developments, making it the most attractive choice for carriers these days.

Along with the better Quality of Service (QoS) offered by LTE, another main driver for this recommendation is the likely 2G and 3G networks phase out within the next decade. According to the Machina Research [17]: “By 2020 it will become increasingly difficult to guarantee 3G network availability in developed markets and by 2025 it will be almost impossible”.

The current disadvantage of LTE is its lower coverage, but PLMN operators are investing massively to enhance it. It is expected that LTE coverage will be in a few years in same level as 2G and 3G today using, e.g., LTE-800 technology. Moreover, development efforts are put on (trusted/untrusted) WiFi-LTE integration to enable more flexible licensed and unlicensed network configurations.

Fixed line technologies, like Digital Subscriber Line (DSL), VDSL, Television (TV) cable and leased lines, are an option for WAN communication in case physical networks are available or the effort needed for its deployment is justified. The main benefits of fixed line technologies, compared to current PLMN, are the higher bandwidth and the absence of interferences. A use case for fixed line technologies is the connection of collection points which have by nature a higher bandwidth demand.

Combining multiple access types is both possible and common in current deployments. Examples could be a router with wireless access on the WAN side and wire in LAN side; or the TV cable as WAN access technology towards a building and PLC for connectivity within the building.

Even if **Power-Line Communication** (PLC) may not be operated by telecom companies, this technology should be mentioned as a way to improve mobile and fixed line network applications and it could be considered for utilities as a special case of fixed line access. PLC can offer a mesh local area network (LAN) to collect a number of smart grid devices towards a WAN access point. The WAN technology could be a mobile network (e.g. LTE) or fixed line. In the case that a high redundancy is required, a PLC LAN could be connected via more than one WAN access point and technology.

PLC could also be used to fill the gap between the location of smart grid devices and a point with mobile (e.g. LTE) coverage. The main benefit is the fact that a communication can be provided without setting up a new infrastructure.

Mesh networks have specific requirements for **address assignment functions**. For future readiness, the IPv6 should be the first choice. The IPv6 offers auto-configuration and standardised functionalities to assign an IPv6 prefix, i.e. range, to a segment behind the LTE or fixed line access point (e.g. to a LAN). Once the IP range is received, all devices inside the segment now in which LAN segment they are. Then, using the address auto-configuration, every device could generate its unique IP host address and be able to communicate inside the LAN and in the WAN.

After IP addresses have been assigned to devices, the next important building block in the Telecom chain is the offering of a **Virtual Private Network** (VPN) inside a Telecom Multiprotocol Label Switching (MPLS) network. This dedicated VPN provides additional security on IP level and gives the utility the freedom to select IP ranges.

In addition to basic transport requirements, the smart grid has also **QoS requirements**. A number of critical communication scenarios are defined with higher QoS, to ensure that critical flows are delivered even in PLMN overload situations. Two independent QoS solutions are available in VODAFONE networks:

- **Basic QoS solution based on APN and SIM**: two Customer Service Profiles (CSP) are defined for a critical Access Point Name (APN), one with normal QoS profile and one for critical traffic with higher QoS. The utility can switch the SIM to select the correct CSP.
- **Enhanced QoS solution based on dedicated bearer**: splitting uncritical and critical flows inside the same APN through different bearers requires setting a prioritised dedicated bearer for critical flows in parallel to the default bearer (for the remaining traffic).

Another key aspect of smart grids is **security**. End-to-end security at the application level is one part, but more security and privacy functions need to be used to harden the communication solution:

- **Security**:
  - **Wholly owned end-to-end infrastructure**: multiple layers of protection built in across the entire value chain.
  - **Protecting data and SMS services**: private IP address, unique APNs provided, private SMS centre.
  - **Internet access**: Access Control List (ACL) avoids fraudulent SIM usage and protects from internet attacks.
  - **SIMs**: In-built cypher keys and authentication.
- **Data privacy**:
  - **Encryption**: end-to-end data encryption, data is sent over private networks.
  - **Data management**: high level data security, compliant with EU privacy directive.

9.2 Internet of Things (IoT) technologies

The concept of **IoT** [18] refers to the network of physical objects, which are able to interoperate within the existing internet infrastructure, where each device is identified through an IP address and where human interaction is not required. The Machine-to-Machine (M2M) data that is exchanged refers normally to the status of devices and measurements from sensors, while "the cloud" provides the administrative user interface and the data analytics functions.

Current mobile networks are, in most cases, poorly suited for low data rate, low power, cheap, battery-operated devices. The Internet of Things has sparked a number of new protocols to serve low data rate applications with likely more uplink (from the thing/edge to the gateway) than downlink, in contrast to mobile broadband systems, which have more downlink than uplink capacity.

Services that leverage **Low Power Wide Area Network** (LPWAN) technologies require mainly deep / wide coverage, low power consumption and massive connections. Low power consumption is a prerequisite for almost 80% of all LPWAN use cases, ranging from applications like smart meter, smart parking, and wearables to smart grid. The cost of these technologies is expected to be lower than that of other "conventional" communication technologies.

GPRS [15] was one of the first networks used for low data rate services. Being part of a mobile network, the nodes send frequent requests to find the adequate base station and, therefore, it uses a non-negligible part of its transmission capability for signalling. Tracking is worth when mobility is required and, conversely, when the end device is stationary and low data rate communication is needed, tracking ceases to be worth.

Since then, **3GPP** has started working groups and has defined a machine (or thing) alternative of its, otherwise, high data rate LTE protocol. Three separate tracks are being standardized in 3GPP for licensed cellular IoT technologies [19], all of them updated in 2016 under Release 16 of the global 3GPP standard: **eMTC** (enhanced Machine-Type-Communications) also known as **LTE-M**, **NB-IoT** and **EC-GSM-IoT**. The first two are based on LTE and the latter on GSM technologies. A 5G solution is expected to be part of the new 5G framework by 2020.

Among the most deployed non-3GPP protocols are **Xbee** [20] and **DASH7** [21] [22]. They have been conceived, from the start, as low power devices sending few bits of information occasionally, mostly as an uplink, to a gateway and the core system. Additionally, other network protocols such as **SigFox** [23] and **LoRa** [24] have been developed, in order to increase range and serve operations over a wider area.

LPWANs are designed for non-time critical applications like metering, location tracking and sensors. Latency is in seconds and this fact limits to certain services their capabilities in smart grids.

In Figure 9.1, the IoT is represented by ZigBee and 6LoWPAN technologies. Low-Rate Wireless Personal Area Networks (LR-WPANs) are specified by the IEEE 802.15.4 standard, which deals with the physical layer and Media Access Control (MAC) in the data link layer. ZigBee, and 6LoWPAN (it allows IPv6 packets to be exchanged over LR-WPAN, network layer) plus standard internet protocols, are two options of covering the rest of layers not specified by the previous IEEE standard.

Many attempts exist in the literature to **compare** the different technologies, e.g. [25]-[27], and Table 9.2 below represents such an exercise. This is a difficult exercise, because much of the key performance indicators are both situation-dependent and usually not independent from each other. For instance, data rate, range, power and costs cannot be optimized simultaneously, e.g., for a fixed transmission power, you get either a long range or a high data rate.

A short explanation of the most important metrics is given hereafter in order to understand the figures presented in Table 9.2:

- **Frequency**: LTE-M is set to operate in the cellular, licensed bands. Conversely, most of the LPWAN protocols (these include but are not limited to; XBee, SigFox and LoRa) operate in the unlicensed 2,4 GHz band (also known as industrial, scientific, and medical – ISM - band), just as Wi-Fi does (2,45 and 5,8 GHz bands, both unlicensed). DASH7, Sigfox and LoRa use unlicensed spectrum under 1 GHz left by the shift from analogue to digital television. In unlicensed bands, interferences are more likely to occur, resulting in unreliable, unstable service. In addition, the 2,4 GHz band and 868 MHz band will be threatened by adjacent cellular operations, causing some extra interference. Inside these internationally regulated frequency bands, each technology uses channels of different sizes, opening up for variations about data rates and vulnerability to interference. Smaller channels mitigate the effect of noise (e.g., Sigfox), while larger ones may need adaptive coding gain to compensate for

variations (e.g., LoRa). Larger channels open up for larger data rates for the same transmitted power.

- **Range and topology**: range in any radio system is subject to several factors including the propagation environment, the transmitted power, the frequency, the modulation type, access method, etc. Therefore, there is usually a bracket of possible ranges, with the "up to" achieved on rare occasions. In addition, topology can help compensate a lack of range through, e.g., a tree structure that repeats and transports the signal one hop further, or a mesh architecture that does not require a central entity. Some technologies exist only in star topology with edge nodes around a single gateway, while others also have mesh capability and possible combinations thereof (e.g., DASH7). 3GPP technologies claim to provide international coverage and well established ecosystems. They are a natural preference for network operators, since they can be installed on existing infrastructure.
- **Transmitted power**: higher transmission power will lead to higher data rates or larger range. Europe and USA have different regulatory regimes and values for allowed transmitted power. Theoretical range is a result of the combination of transmitted power, modulation type and access method. Yet, an important factor in wireless systems is interference from neighbouring radio transmitters, which can substantially limit range, see next paragraph.
- **Interference**: interference happens at physical level where (rather cheap) receivers try to sort interesting signals from the surrounding noise, caused by other transmitters in the vicinity. Consequently, an ideal range is reduced in a noisy environment. Blockage by walls, vehicles, even people also alters range. This causes the difference between an "up to" range and "typical" range.Additionally, different transmitters try to access the system and get a channel concurrently. In order to avoid collisions, one can use collision avoidance techniques following the principle: “listen, then talk.” This means that there must be a receiver capable of listening (downlink) before the device gets to talk (uplink). Early systems (e.g., at Sigfox) were uplink-only, in order to save costs on the receiver equipment and power consumed for listening and synchronizing with the gateway. Another strategy consists in transmitting and waiting for acknowledgement. If the latter does not come, one assumes collision and resends data according to a back-off algorithm (collision detection mechanism, e.g., Aloha protocol). Protocols that do not infer collision avoidance or detection run the risk to saturate the network, and may have to limit a priori the data rate in order to regulate the entry into the network access (e.g., Sigfox policy).
- **Mobility**: GPRS and LTE-M are mobile technologies, in contrast with the rest of the technologies considered here. Although it is at an early stage for LTE-M, and roaming agreements for LTE-M SIM cards have not yet been addressed, the possibility lies for both mobile and international IoT services. Mobility is ensured through handovers, where the edge devices signal is tracked and relationship to the base station (gateway) is established, while

having constantly a list of neighbouring base stations the device can be connected to in case of a more preferable location. This process consumes network signalling resources, both on the uplink and downlink of the radio link.

- **Energy consumption**: An important metric for LPWAN is the energy consumption, because the end device may be battery-operated. The energy consumption is especially important at the edge of the network, since a service turns profitable only if the battery remains unchanged for, typically, several years. Many factors affect the energy consumption, including but not limited to, the modulation technique, media access protocol, acknowledgement with the gateway, possible adaptive techniques, mobility and tracking, and duty cycle. Low duty cycles allow the devices to be in sleep mode for a long period and awake only for transmitting data. The power used to transmit data is also an important factor that will vary according to technology, range, and usage period. A high power for a short time can lead to great longer sleep mode periods and extended battery life.
- **IP**: The Internet Protocol (IP) forms the backbone of connectivity for WAN networks. This simplifies connectivity and allows the use of a wide range of low-level communication technologies without having to deal with implementation details below the network or transport layers. Not all technologies, however, are compatible with IPv6, which casts doubts about their longevity. IPv6 stands as a long-term solution not only in terms of IP range but also for its key capability to strengthen security.
- **Cost**: The more complex is the edge node, the higher is the cost for the service provider. A simple Sigfox or GPRS node is substantially cheaper than that of other competitors. But in order to compare costs of different systems, one has to take into account the cost of the edge nodes, the gateway, and operational costs. With technologies relying on public service like those of 3GPP (GPRS, LTE-M) or deployed in partnership with telecommunication operators (Sigfox and, up to some extent, LoRa), the end customer pays for the edge node and service operation, while the operator pays for the backhaul infrastructure. Conversely, the other networks are run on a private ownership model, where the service provider pays for the whole chain.

Below, an attempt to summarize and compare different parameters is shown in Table 9.2.

Technology	GPRS	LTE-IoT	Sigfox	LoRa	Wi-Fi 802.11ah	X-bee	DASH7
Frequency	8-900 MHz licensed	7-900 MHz licensed or shared	ISM; 868 / 902 MHz	ISM; 433/868(EU) 780/915 (USA) 902 MHz	Unlicensed under 1GHz, except TV	900 MHz, 2.4 GHz	ISM; 433/868(EU)/ 915 (USA) MHz
Channel width	200 kHz	1.4 MHz and 200 kHz (NB version)	100 Hz	≥125 kHz	1/2/4/8/16MHz		25 or 200 kHz
Modulation Access technique	Time division multiple access	Frequency division multiple access (UL), Orthogonal frequency division multiplex(DL)	Binary phase-shift keying	Frequency shift keying + Chirp spread spectrum	Time division multiplexing / Orthogonal frequency division multiplexing	Spread spectrum	Frequency shift keying + Carrier sense multiple access
Transmitted power (edge)	Up to 43 dBm	100 mW (=20 dBm)	Up to 100 mW (=20 dBm)	EU: 14 dBm, US: 27 dBm	1 mW-1 W (30 dBm), depending on region	1 mW-100mW (cap 10 mW=10 dBm in EU)	433 MHz: +10dBm 868/915 MHz: +27dBm
Range (typical)	5 km	2-5 km (rural)	10 km (urban), 100 km (rural)	5 km (urban), 15 km (rural)	1 km (rural)	30m-1km	5-10 km
Topology	Star	Star	Star	Star	Star, tree (2-hop)	Star, mesh	Star, tree, mesh
Data rate DL	10 kb/s	150 kb/s (NB) < 1Mb/s	4x8b/day	EU: 30 b/s-50kb/s US: 100-900 kb/s	150 kb/s, up to 300 Mb/s	9.6-250 kb/s	9.6-167 kb/s
Data rate UL	10 kb/s	150 kb/s (NB) < 1 Mb/s	100 b/s	EU: 30 b/s-50kb/s US: 100-900 kb/s	150 kb/s, up to 300 Mb/s	9.6-250 kb/s	9.6-167 kb/s
Mobility	Yes	Yes	No	No	No	No	No
# nodes per gateway	5000	50000	1000000	250000	8191	50000	N/A (connectionless)

Technology	GPRS	LTE-IoT	Sigfox	LoRa	Wi-Fi 802.11ah	X-bee	DASH7
Duplex mode at gateway	Full	Full	Half	Half	Full	Half	Half
Battery life (estimated given duty cycle)	1 week	5 years	10 years	10 years	1 week	10 years	10 years
Support for IPv6	no	yes	Unlikely	Likely	Likely	likely	Likely
Governing body	3GPP	3GPP	Sigfox	LoRa alliance	Wi-Fi alliance and IEEE standards	Wi-Fi alliance and Digi	DASH7 alliance
Deployment status	Deployed for several decades	Planned	Deployed since 2009	Planned	Planned	Deployed	Deployed since 2015
Costs (est., in $)	Node: 2	Node: 5	Node: 2	Node: 30	Node: 5	Node: 5	Node: 2

Table 9.2 Comparison of LPWAN systems

10 Appendix B: Information standards and protocols

The services and functionalities carried out for smart grid operation imply information exchange among different components (business actors and systems). The characteristics of this data set requirements for communication and computational capabilities of smart devices and backend systems. Some of the **features** to be considered on information to derive requirements are the following:

- Size of each information exchange, which depends on the type of signal to be exchanged (on/off, energy price, bid, metering data, etc.) and, therefore, on the characteristics of the protocol or standard that defines it.
- Frequency of the information exchange.
- Latency thresholds of the information exchange.
- Data flow direction: one or two ways.
- Security level.

Some of the most important standards and protocols in the smart grid environment, according to the CEN-CENELEC-ETSI Smart Grid Coordination Group SG-CG [3][5], have been analysed, in order to understand the already defined data models that might be used for information exchanges leading to network services provision. This knowledge allows us to match requirements to existing developments or/and to identify gaps according to the needs of the project.

A short description of the main standards is provided later in this section. Together with the candidate standards for smart grids, some other protocols have been reviewed. The data types covered by the standards have been extracted and summarized in the following Table 10.1. They can be classified in accordance to the following smart grid fields:

- **Distributed Energy Resources (DER) integration**: data types permitting to include small capacity systems as flexibility resources in the network: distributed generation, storage and Demand Response (DR). They can be signals for the direct control of load, generator and/or storage, price schedules to induce customer change their consumption habits, etc.
- **Energy market participation**: data types that permit the participation of players in energy market processes (procurement, activation, settlement, etc.).
- **Network Automation**: data formats that transmit information allowing network operation through the control, monitoring, etc. of network devices and processes.
- **Backend application integration**: data models permitting the data exchange between backend applications supporting the management of electricity networks (basically, based on CIM).
- **Advanced Metering Infrastructure (AMI) and Automatic Meter Reading (AMR)**: metering information related data exchanges.

Type of data to be exchanged	Field	EI	EDI	IEC 60870-5	IEC 60870-6	IEC 61850	IEC 61968	IEC 61970	IEC 62056	IEC 62325	IEC 62746-10	SEP 2.0
1- Availability schedule for service participation	DER											
2- Registration / enrolment for services												
3- Price bid												
4- Power / energy bid												
5- Price signal / schedule												
6- Power / energy settings												
7- Event/service definition and activation												
8- Event/service verification												
9- Market context definition	Market											
10- Market document / messages exchange (secure)												
11- Market business process implementation methodology												
12- Capacity allocation and nomination: congestion management and scheduling												
13- Acknowledgement of business process in markets												
14- Scheduling information												
15- Reserves resources information: tendering planning and activation.												

Type of data to be exchanged	Field	EI	EDI	IEC 60870-5	IEC 60870-6	IEC 61850	IEC 61968	IEC 61970	IEC 62056	IEC 62325	IEC 62746-10	SEP 2.0
16- Settlement data (imbalance reports, metered information, finalized schedules...)												
17- Problem settlement and status request in market processes												
18- HVDC scheduling												
19- Information for interconnection capacity determination from critical network elements												
20- Device monitoring information	Network											
21- Device control signal												
22- Inter-control centre information												
23- Distribution system and business properties (inter-control centre)	Enterprise											
24- Transmission system and business properties (inter-control centre)												
25- Metering	AMI											

Table 10.1 Data types in ICT standards and protocols

The fields above are mapped to the Smart Grid Architecture Methodology (SGAM) zones and domains in the following Figure 10.1.Basically:

- **Distributed Energy Resources (DER) integration**: it corresponds to the DER and customer premises domains and involves mainly from station to enterprise zones.
- **Energy market participation**: it involves the market and enterprise zones for all domains.
- **Network operation**: it is linked to the Distribution and transmission domains but involves also DER and customer infrastructure, from operation to process zones.
- **Enterprise processes**: it involves the enterprise and operation zones for all domains.
- **Advanced Metering Infrastructure (AMI) and Automatic Meter Reading (AMR)**: It involves customer premises, from operation to process zones.

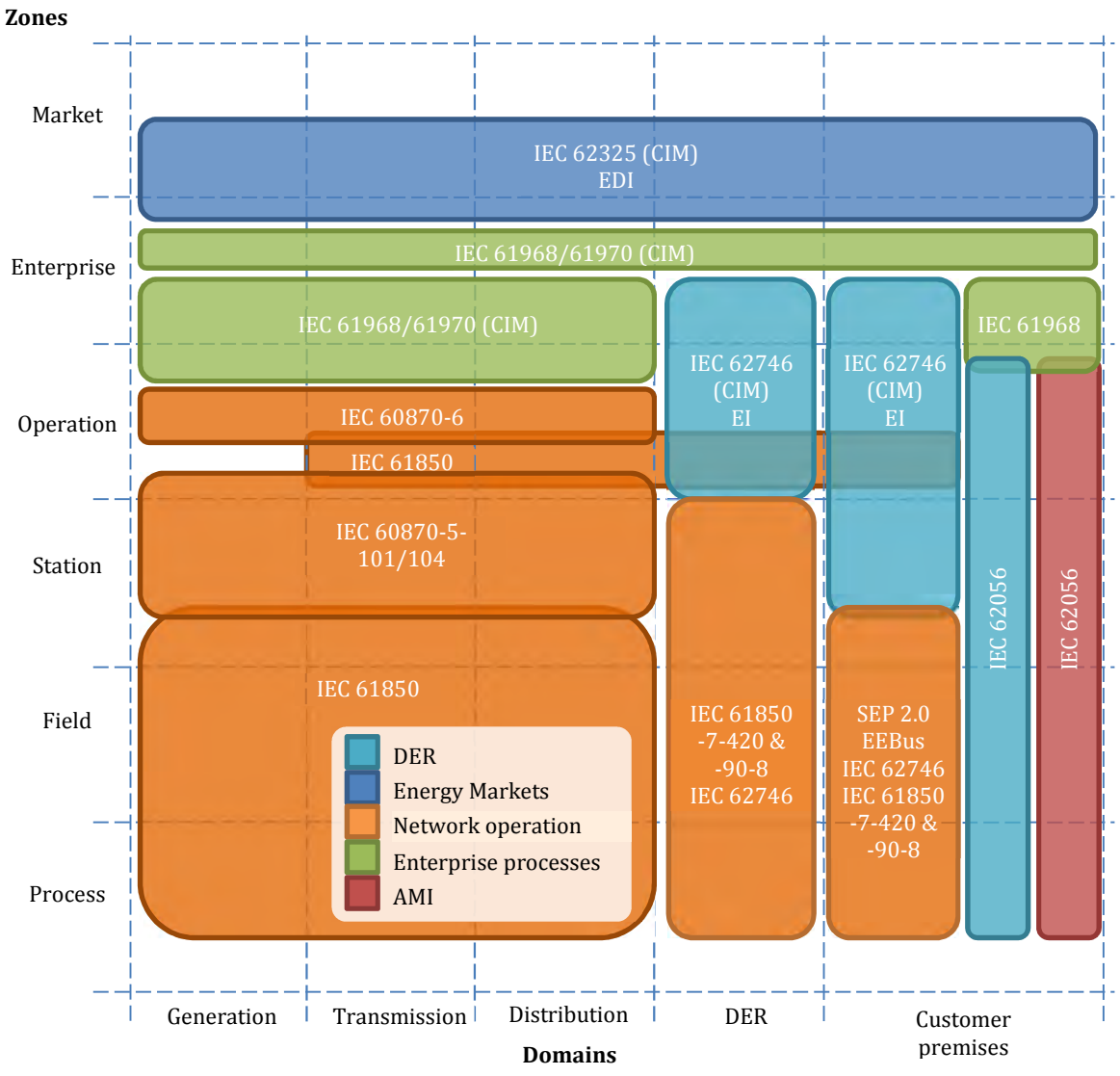


Figure 10.1 Mapping of data types to the SGAM zones and domains

10.1 Energy interoperation

The Energy Interoperation (EI) [28] defines the interaction between the Smart Grids and their end nodes (such as smart buildings, companies, industry, homes and vehicles). This interaction is designed as SOA (Service Oriented Architecture), which allows that any system can be easily integrated and deployed.

The EI is an OASIS standard which includes data and communication models which enable the message exchange for dynamic pricing, reliability, and emergencies. These two models (Information Model and Communication Model) enable collaborative and transactional use of energy, service definitions and vocabularies for the interoperable and standard exchange of:

- Dynamic price signals.
- Reliability signals.
- Emergency signals.
- Communication of market participation information such as bids.
- Load predictability and generation information.

This work facilitates enterprise interaction with energy markets, which:

- Allows effective response to emergency and reliability events.
- Allows taking advantage of lower energy costs by deferring or accelerating usage.
- Enables trading of curtailment and generation.
- Supports symmetry of interaction between providers and consumers of energy.
- Provides for aggregation of provision, curtailment, and use.

EI is at version 1.0 and the latest edition of its specification was released in June 2014. This is a relatively new standard, so it includes services, descriptions, signals and messages for many elements that are present in the Smart Grids nowadays. It is defined to work as services, which enables that any element in the Smart Grid can publish its functionality as services, allowing other elements or systems to use these services.

The technological solutions this standard provides are mature and widely adopted not only by companies, which have servers with high computational features, but also by DERs with low performance chipsets:

- **XML for the Information Model**: the data is exchanged using XML (eXtensible Markup Language), where the data composition follows the rules defined by its XSD (XML Schema Definition).
- **Web Services for the Communication Model**: when a system needs access to a resource, it invokes the service (as any client/server architecture).

The main advantage of this technology is that it uses WSDL (Web Service Description Language) to describe a service and its operations and SOAP (Simple Object Access Protocol) to transport the messages.

Any implementation may provide extension(s) to the standard, whether of information structures, services, service operations, or payloads, but these extensions must be documented in the implementation conformance statement.

The EI defines a set of data models to contain information and to define the structure that must be used when it is transmitted. In the following paragraphs the complete set of services is described along with the data structures they contain.

10.1.1 Market Context Services

Each event and service in EI takes place within a Market Context. This Context defines the behaviours that that each Party can expect from the other. Market Contexts are used to express market information that rarely changes, and thereafter not need to communicate it with each message.

10.1.2 Availability Services

The Availability is set by the Virtual End Node (VEN) and indicates when an event may or may not be accepted and executed by the VEN with respect to a Market Context. Knowing the Availability and Opt information for its VENs improves the ability of the Virtual Top Node (VTN) to estimate response to an event or request. The availability data structures (EiAvailability) describe only the availability times using calendar patterns.

10.1.3 Services to temporary enable/disable the availability

When a VEN enrols in an event-oriented Market Context, it makes itself Available to respond to events on a given schedule. The Availability schedule may be simple (all day, all the time) or complex (weekday afternoons, on weekends with a long notice, and not on Thursday mornings during biweekly payroll). No matter how simple or complex the Availability, the VEN may choose to change it for a limited period. This decision is communicated with an Opt (as in “Opt Out” for temporally not applying the availability and “Opt In” to apply the availability again).

As a result, the Opt service creates and communicates Opt-In and Opt-Out schedules from the VEN to the VTN. Schedules are combined with EiAvailability and the Market Context requirements to give a complete picture of the willingness of the VEN to respond to the events received by the VEN.

10.1.4 Transactions

Transactional Services define and support the lifecycle of transactions inside an overarching agreement, from initial quotations and indications of interest to final settlement. The phases are:

- **Registration**: designed to enable further phases. The Register Party service operations create a registration for potential Parties in interactions. This is necessary in advance of an actor interacting with other parties in various roles such as VEN, VTN, tenderer, and so forth.
- **Pre-Transaction**: Pre-transaction services are those between parties that may or may not prepare for a transaction. The services are Tender and Quote. A quotation is not a tender, but rather a market price or possible price, which needs a tender and acceptance to reach a transaction. Price distribution, which is sometimes referred to as price signals, is accomplished using the Quote and Tender services. Quotes are indications of a possible tender price; they are not actionable. A Tender offers prices at which Transactions may be made; they are actionable.
- **Transaction Services**: These operations manage the exchange of transactions. For example, in demand response, the overarching agreement is the context in which events and response take place, what is often called a program. This agreement is identified by the information element Market Context here and elsewhere. Notice that there is no way to cancel or change transactions, it is due to as in other distributed agreement protocols, a compensating transaction should be created as needed to compensate for any effects.
- **Post-Transaction**: In a simple market, verification would be solely a function of meter readings. However, in today's markets, with most customers on Full Requirements (Full Requirements describes the situation where purchases are not committed in advance) tariffs, the situation is more complex. The seller is generally obligated to provide all that the buyer requires. Full requirements tariffs create much of the variance in today's DR markets. These sections will apply a measurement model consistent with the data model defined in the EiReport Services.

For transactional services, the roles are Parties and Counterparties. For event and resource services, the Parties adopt a VTN or VEN role for interactions. The register services identify the parties for future interactions. This is not the same as (e.g.) a program registration in a demand response context. Here, registration can lead to exchange of tenders and quotes, which in turn may lead to a transaction which will determine the VTN and VEN roles of the respective parties.

10.1.5 Enrolment services

Enrolment is distinct from Registration in EI. Registration establishes an identity for an actor (a party or a device such as a generator or a meter on a premise). Enrolment establishes a relationship between two actors as a basis for further interactions. Energy Interoperation supports two classes of interactions; Transactional and VTN/VEN interactions.

- **Enrolment in Transactional Interactions**: the enrolment service identifies the two parties and the Enabling Agreement, Market, Tariff, Purchasing, Selling, etc. that the parties agree to use for their interactions.
- **Enrolment in a VTN/VEN Interactions**: the enrolment service identifies the two actors, generally a registered Resource and a Service Provider acting as a Designated Dispatch Entity (DDE). Registration of a Resource may sometimes be automatic with enrolment of the Resource.

10.1.6Events

The Event Service is used to call for performance under a transaction. The service parameters and event information distinguish different types of events. Event types include reliability events, emergency events, and more; and events may be defined for other actions under a transaction. For transactional services, two parties may enter into a call option. The event based interactions are defined through the following items:

- **Event Descriptor**: it contains metadata about the event nature, including the ID, the priority, the market context which manages the event, the status, date of creation and modification.
- **Event Active Period**: it is a sequence that describes the overall schedule for an Event. The Active period is of Vcalendar type (also described in OASIS) that contains a Sequence and may have its own properties. The Sequence of an Active Period generally falls into a common Interval pattern of Notification, Ramp-up, Active, and Recovery.
- **Event Signals**: they convey the detailed information about the schedule for an event. When an Event conveys multiple signals (stream of signals), they may be aimed at different target resources in different Market Contexts, or they may use different semantics, i.e., one use Price and another use Simple Level semantics.

Units	KW	Start:	8:00	Duration:	1Hour	Quantity	10
				Duration:	1Hour	Quantity	10
				Duration:	1Hour	Quantity	15
				Duration:	1Hour	Quantity	25
				Duration:	1Hour	Quantity	10

Figure 10.2 Power sequence basic example using EI (from EMIX)

- **Baselines**: baselines are streams that can incorporate signals and share many of the same elements. As some signals indicate the performance requested is relative to that in another interval, Baselines indicate the performance in that Interval.
- **Enabling choices**: they can be used by the VEN to temporarily modify availability in the pre-existing agreement.

A single Event may be broadcast to many VENs with similar performance characteristics. If the VENs all perform in unison, it can create spikes (or sudden drops) in energy use that can be harmful to the distribution system. It is necessary for a VEN to be able to ameliorate this issue by requesting response smoothing, also covered by EI using time restrictions, intervals, tolerances, etc.

10.1.7Reports Services

Energy Interoperation Reports convey information from remote sensing or about remote state back to the requester. The Historian operations support the collection of data for Reports, which can be associated with an Event or can be requested on demand. The general pattern of the Report service is to request historical data, or to serve the Report when it is ready.

10.1.8Profiles

A profile includes a selection of interfaces, services and options for a particular purpose. Three normative profiles are part of EI 1.0:

- **OpenADR** (for more details, see section 10.10 in this annex): it defines the services required to implement a similar functionality to that of OpenADR. It updates and gives a broader applicability to the so called "2 Profile".
- **Transactional eMIX (TeMIX)**: it defines the services required to implement the functionality for market interactions.
- **Price distribution**: it defines the minimal set of services required to interact with a pure price distribution (price signals) context.

10.2 ENTSOE-EDI

The European Network of Transmission System Operators for Electricity (ENTSO-E) maintains an Electronic Data Interchange (EDI) library. The "work products library" [29] contains several documents and definitions approved by ENTSO-E for the harmonisation and implementation of standardised electronic data interchanges in the context of achieving EU Energy policy goals. Subsequently the most relevant in the project's scope are selected and described.

10.2.1ENTSO-E EDI role model

The harmonized role model presented in [30] provides a common definition of roles and domains employed in the electric market. It defines a common language for developers and engineers in the field of information exchange in the energy market. Thereby, one party may (probably simultaneously) act in different logical roles, or the roles may be assigned to an organisation's subunits, e.g. company's departments. Beside the roles, also the different domains, in which the roles may act, are defined. The domains are characterized as a grouping of elements with common characteristics.

The role model as a whole (cf. Cha. 4 in [30]) can be used to identify the SmartNet relevant (sub)system, the involved roles, their interaction and necessary communication paths and data.

10.2.2 ENTSO-E Market Data Exchange Standard (MADES)

The Market Data Exchange Standard (MADES) is comprised of standard protocols and utilizes IT best practices to create a mechanism for exchanging data (documents) over any TCP/IP communication network, in order to facilitate business to business information exchanges as described in IEC 62325-351 and IEC 62325-451 standards.

Objects transported within the MADES network are messages where the sender document is repackaged in a header containing all the necessary information for tracking, transportation and delivery.

The scope of MADES is depicted in the following figure.

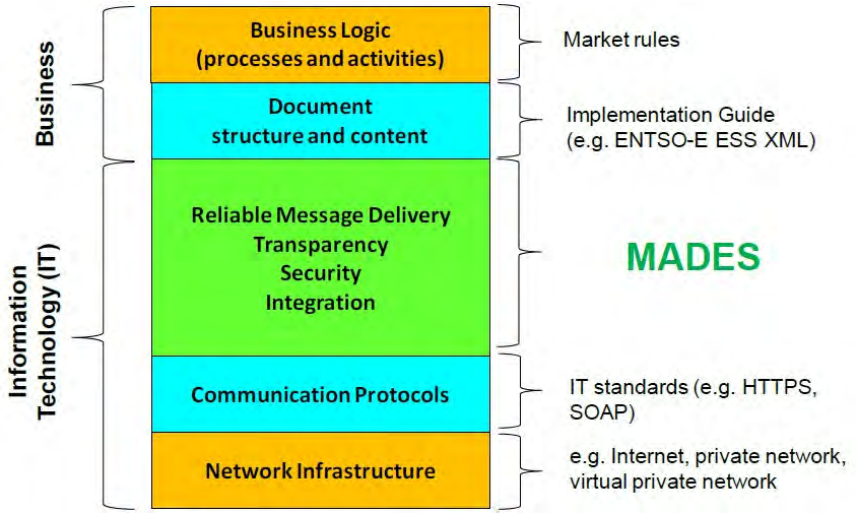


Figure 10.3 MADES scope [31]

10.2.3 ENTSO-E Modelling Methodology for the Automation of Data Interchange of Business Processes (EMM)

The European Transmission System Operators (ETSO) modelling methodology (EMM) [32] aims to be a implementation guide for defined business processes within the energy market. It follows an 8 step process with 5 key milestones and concludes with an implementation guide. As a result the EMM is an implementation guide that can be used by TSOs (or by software developers/providers) to satisfy given business needs.

Below the ETSO methodology outline including its 8 steps and 5 milestones is depicted.

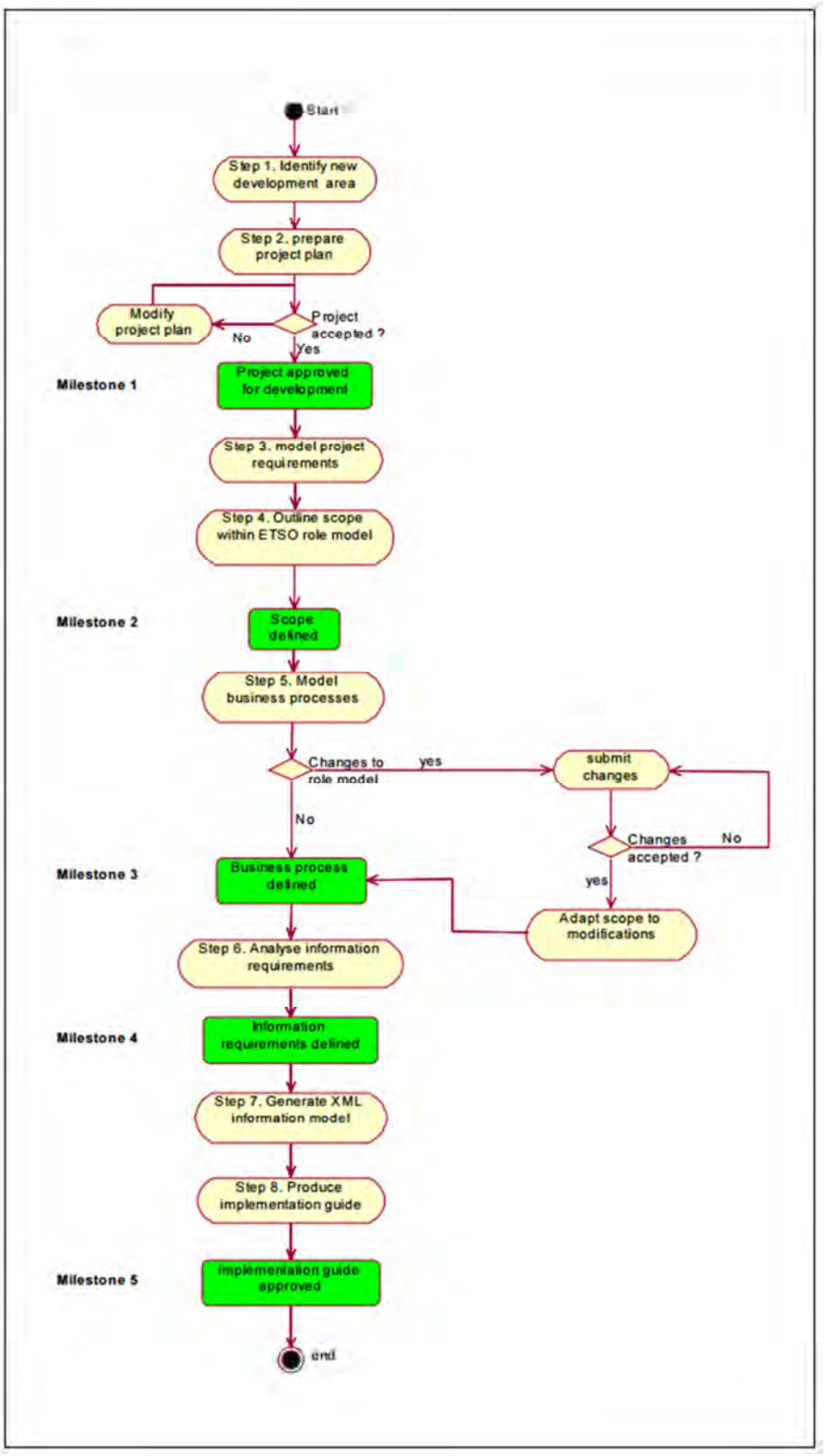


Figure 10.4 ETSO modelling methodology steps

10.2.4 ENTSO-E EDI implementation guides and process descriptions

The several implementation guides and process descriptions are examined subsequently.

The **ENTSO-E Capacity Allocation and Nomination system** (ECAN) [33] is an implementation guide whose aim is to enable IT companies and vendors to develop a software application for market players that can exchange information for transmission capacity right allocations and nominations within the congestion management and scheduling processes. The focus of this implementation guide is to provide the generic information model for the data exchange between the Transmission Capacity Allocator, the System Operators and the various market players who are participating in the capacity market for cross border scheduling.

The **ENTSO-E Scheduling System** (ESS) [34] consists of business-to-business implementation guides for the standardisation of the scheduling process information exchange between Market Participants in the European Internal Electricity Market. It also supports software vendors to exchange electricity market schedules, such as day-ahead and intraday schedules. Information flow and participating roles (according to the Harmonized Role model) are identified for several business cases within the planning phase, not for the operation and not for the imbalance settlement phase. Detailed implementation details are specified and available (primarily) as XSD descriptions.

The **ENTSO-E Reserve Resource Process** (ERRP) [35] allows for software vendors to develop an IT application for market players that can exchange information for reserve resource tendering, planning and activation within the balance management process. Business processes are described covering both technical and commercial aspects of the European system control (UCTE & NORDEL) e.g. primary, secondary and tertiary control. Two different market trading models are covered, which are (a) System Operator - Resource Provider and (b) System Operator - System Operator. For the Resource Reserve Process, the relevant actors and communication paths are identified for both of these market trading models (referred to as use cases) by describing all necessary workflows.

- Tender Workflow.
- Planning Workflow.
- Activation Workflow.
- Tender Reduction Workflow.
- Tender Sharing Workflow.

Consequently, ERRP information requirements are extracted and detailed specifications for the workflow-corresponding documents are created (i.e., Reserve Bid document, Reserve Allocation Result document, Planned Resource Schedule, Resource Schedule Anomaly Report, Resource Schedule Confirmation Report, MOL document, Activation document, and Redispatch Document).

The **ENTSO-E Settlement Process** (ESP) [36] is an implementation guide for software vendors to develop IT applications for market players to exchange electricity market settlement information (e.g.,

imbalance reports, metered information, regulatory data, and finalized schedules). It is based upon an agreed generic imbalance settlement process. Unlike ESS, ESP is relevant after the operation phase to assess the imbalance with a balance area. By UML process flow diagrams, the imbalance settlement relevant data is identified and results in the Energy Account Report specification. A detailed information model with class and element descriptions is presented for the Energy Account Report.

The **HVDC Link Process** [37] has the objective to make it possible for software vendors to develop an application for market players in order to exchange information relative to HVDC scheduling processes.

The objective and scope of the **ENTSO-E Critical Network Element Implementation** [38] is to enable software vendors to develop an IT application for market actors to exchange information between critical network elements used for interconnection capacity determination processes. This implementation guide is one of the building blocks for using UML based techniques in the definition and message process for interchange between different actors in the European electrical industry.

10.3 IEC 60870-5

IEC 60870-5 [39] is a standard widely used in the automation domain and specifically in control of power systems. The standard defines data transmission protocols and a simple ID-based data model. No higher level data model is provided, resulting in the need of so-called interoperability lists, which define the naming of data points in order to achieve interoperability between different vendors or even among products of the same vendor.

The description of the data link framing formats (IEC 60870-5-1) was published in 1990, and the procedures (commands and formats) for link transmission (IEC 60870-5-2) were published in 1992. Many SCADA system suppliers quickly adopted these into their existing products, leading to the emergence of a new wave of protocols that offered essentially interoperable data link framing, but having proprietary application layers. This permitted these suppliers to truthfully state compliance to the standards.

However, most of these protocols remained proprietary, and did not gain wide market acceptance. One notable exception was the Distributed Network Protocol version 3.00 (DNP V3.00) produced by Westronic and placed in the public domain. By taking this unusual step at a time when the IEC standard for the application layer was still far in the future, DNP became an accepted de-facto standard by many equipment vendors in North America. It was not until the release of IEC 60870-5-101 in November 1995 that there was an official international standard application layer for electric power SCADA.

The IEEE's Power Engineering Society has taken an interest in the developments of SCADA protocols and substation automation systems. The IEEE has published a trial use recommended practice for substation data communication (IEEE P1379) that recommends both DNP and IEC 60870-5 protocols as suitable for use.

The protocol stack is based on the reduced reference model called enhanced performance architecture (EPA). EPA includes three layers of the ISO-OSI model:

- **Application layer**: it defines de information elements. The IEC 61870-101 uses the frame format FT1.2, both in fixed and variable length modes. Single control characters are also permitted in this frame format.
- **Link layer**: it defines the frame formats and transmission procedures of the communication. It consists of a number of transmission procedures using explicit Link Protocol Control Information, which are able to carry Application Service Data Units (ASDU) as link user data.
- **Physical layer**: it deals with the hardware-dependent specifications. It uses v.24 and v.28 standards of ITU-T recommendations.

The IEC 60870-5-104 specifies the transport of IEC 60870-5-101 data over TCP/IP.

10.3.1IEC 60870 Overview

The IEC 60870-5 group of standards defines rules and definitions for data presentation and transmission procedures. No rules for application level interpretation of data are provided.

The basic standards IEC 60870-5-1 to IEC 60870-5-5 define the building blocks for definition of individual communication protocols (companion standards, also called "profiles"). The companion standards IEC 60870-5-101 to IEC 60870-5-104 refer to (selected) definitions of the basic standards, which are automatically part of the companion standard.

Companion standards contain "interoperability lists". These lists have to be filled by manufacturers of compatible equipment. Theoretically devices from two different suppliers shall cooperate, if the interoperability list contains the same entries (in real life this is not exactly true).

- IEC 60870-5-1: Transmission frame formats.
    - IEC 60870-5-101: Companion standard for basic control tasks.
    - IEC 60870-5-102: Transmission of integrated totals in electric power systems.
    - IEC 60870-5-103: Communication interface of protection equipment.
    - IEC 60870-5-104: Network access for IEC 60870-5-104 using standard transport profiles.
- IEC 60870-5-2: Link transmission procedures.
- IEC 60870-5-3: General structure of application data.
- IEC 60870-5-4: Definition and coding of application information elements.
- IEC 60870-5-5: Basic application functions.

10.3.2The IEC 60870-5-104 companion standard

IEC 60870-5-104 is widely used in power system automation over WANs today.

The IEC 60870-5-104 profile is an exception to the rule for building companion standards from the IEC 60870-5 group. Instead of using link layer definitions (from IEC 60870-5-1 and 60870-5-2), transport profiles of standard (WAN) technologies are utilized. This is the major reason for its wide use. However, the higher level protocol layers are the same as in the 60870-5-101 standard.

The interface between "IEC-101 application" and the TCP/IP protocol stack is not defined in detail. Appropriate interface libraries exist in nearly any operating system like UNIX, VxWorks, WindowsNT, LINUX, etc. The 104-profile requires the functionality "open", "close", "send" and "receive". Optimized setup of the TCP/IP and underlying layers is not part of the profile (must be handled separately).

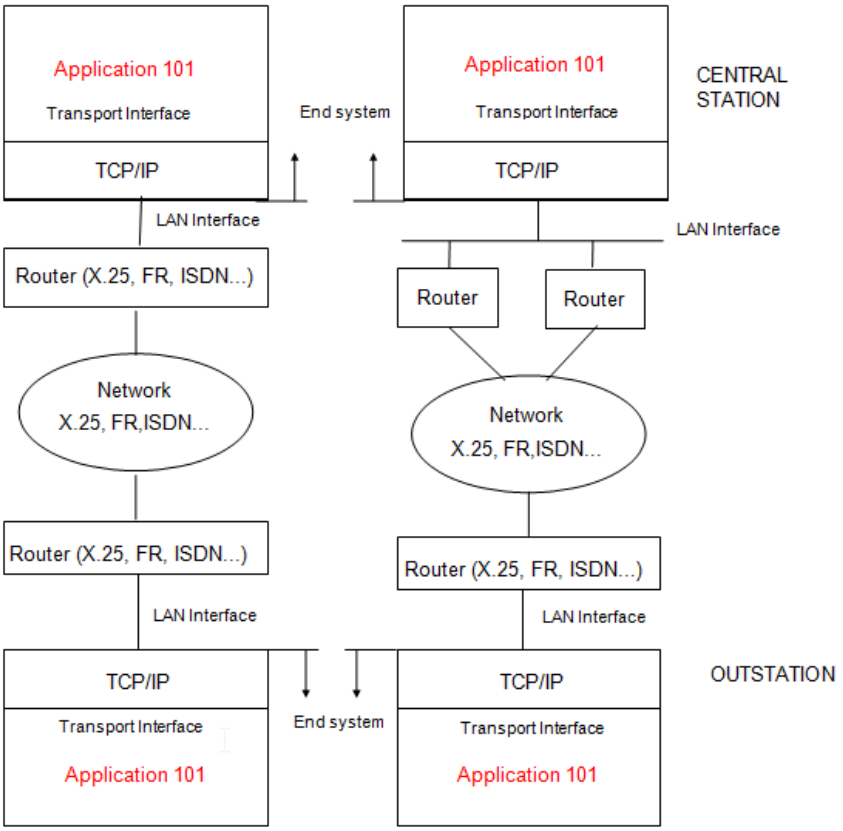
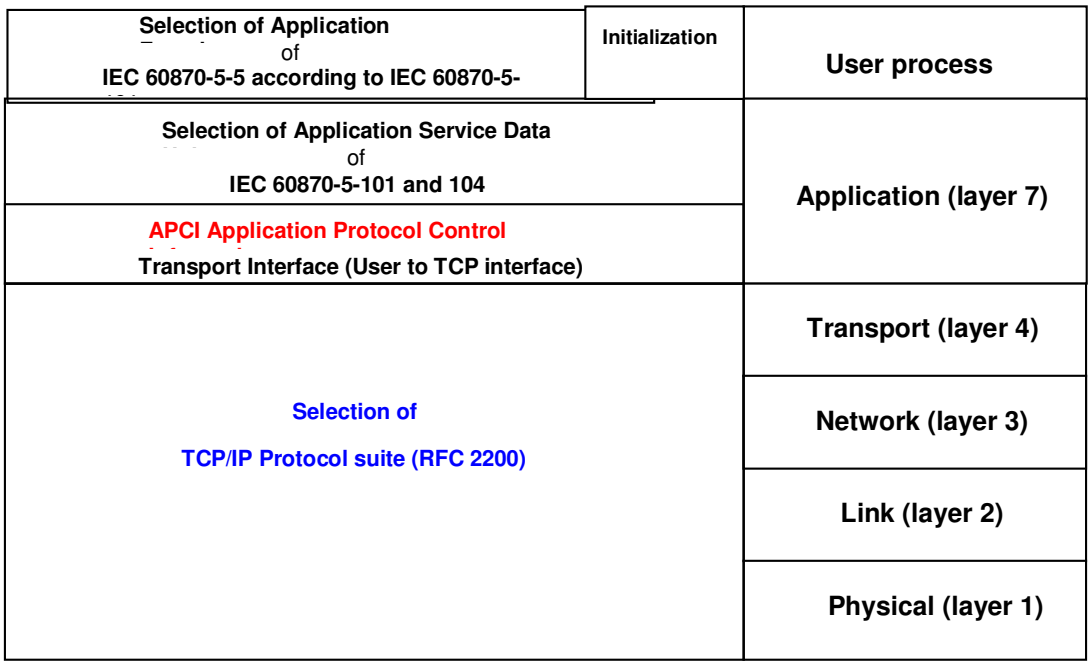


Figure 10.5 IEC 60870-104 general architecture examples (without, left, and with redundancy)



Note: Layers 5 and 6 are not used

Figure 10.6 IEC 60870-104 architecture

10.3.3IEC 60870-5-5 (Basic application functions)

This standard defines procedures for handling application level functions according to the Enhanced Performance Architecture (EPA) reference model. Companion standards refer to these basic procedures and therefore do not contain their own procedure descriptions for the standardized parts. The basic procedures may be mixed on one link, but only different procedure types (example: a command procedure may be executed while a general interrogation is running, but a command procedure must not be interrupted by another command procedure). Availability of the required link services is a precondition for implementation of the basic application procedures.

These are the **basic application procedures**:

1. Station initialization.
2. Data acquisition by polling.
3. Cyclic transmission.
4. Acquisition of events.
5. Quick-Check (not used for the IEC companion standards).
6. General interrogation, station interrogation.
7. Clock synchronization.
8. Command transmission.
9. Transmission of integrated totals (counters).
10. Parameter functions.

11. Test procedure.
12. File transfer.
13. Acquisition of transmission delay.

The basic application procedures generally describe exchange of Application Service Data Units (ASDUs) between two applications. Within IEC 60870-5-5 all ASDUs are identified by symbolic names. The rules for construction of these names are also valid for all companion standards.

Examples for symbolic names: M_ME_NA_1, M_SP_TB_1

- M: identifies the general type of ASDU (M = monitor information, C = control information, P = parameter, F = file transfer).
- ME: identifies a certain data type (examples: ME = measured value, SP = single point).
- N: identifies use of time tags (N = no time tag, T = with time tag).
- A: identifies the individual sub-types of a data type (A, B, C, etc. every companion standard has its own definitions).
- 1: identifies the companion standard, for which the definition is valid (1 = 101, 2 = 102, etc.).

10.4 IEC 60870-6 (ICCP)

The IEC 60870-6 standard (also known as TASE.2 or ICCP) specifies a method of exchanging time-critical control centre data through LAN and WAN networks. It contains provisions for supporting both centralized and distributed architectures. This standard includes the exchange of real-time data indications, control operations, time-series data, scheduling and accounting information, remote program control and event notification [39].

ICCP (Inter-Control Centre Communications Protocol) provides real-time data exchange between energy companies by means of a client-server architecture, where any company can initiate a connection. The message exchange consists of requests for information and control signals. The field devices in the domain of control of the Company A can be included in the domain of control of the Company B to create an inter-domain control area. This way, ICCP enables to extend from local monitoring and control to an inter-SCADA environment.

IEC 60870-6 has been present for several years and has been evolving until the present 2014 ICCP release. Current versions include:

- Services and Protocol (IEC 60870-6-503).
- Object Models (IEC 60870-6-802).
- Application Profile (IEC 60870-6-702).

ICCP uses a well-proven, robust, existing standard called the Manufacturing Message Specification (MMS) for the messaging service which was designed to facilitate the exchange of real-time application to address the needs of the industry sectors.

As MMS is an object-oriented program, which allows organizations to structure discrete objects incorporating both information and behaviour. As a result, MMS is relatively easy to implement and maintain. However, the data models have been defined to 'run' within the standard defined communications. This means that the current systems (SCADA, Control Centers, RTUs, etc.) which are currently operating under the IEC 60870 series are ready to use it, whereas other systems will have more difficulties to adopt them.

Supported data types defined in the ICCP Object Models (IEC 60870-6-802) include control messages, status, analogues, quality codes, schedules, text and simple files. In addition, optional functions include remote control, operator station output, events, and remote program execution.

This part of the IEC 60870 specifies a method of exchanging critical control centre data through wide-area and local-area networks. It supports both centralised and distributed architectures and includes the exchange of:

- **Real-time data indications**.
- **Control operations**.
- **Time-series data**.
- **Scheduling and accounting information**.
- **Remote programme control and event notification**.

Though the primary objective of this protocol is to provide control centre (telecontrol) data exchange, its use is not restricted to control centre data exchange. It may be applied in other domains such as power plants, factory automation, process control automation, etc.

A control centre includes four primary **classes of host processors**, normally connected through one or more LAN:

- **SCADA/EMS**: monitoring is performed via Data Acquisition Units and Remote Terminal Units.
- **Demand Side Management (DSM)/Load management**.
- **Distributed applications**: they perform miscellaneous analysis, scheduling or forecasting functions.
- **Display processors**: they allow for local operator and dispatcher display and control.

The control centre will also have access to several WANs. These WAN connections may include the company-wide area network for communications with the corporate host and a distinct real-time SCADA network. Each control centre will also have one or more TASE.2 instances to handle data exchange with remote control centres.

The TASE.2 protocol relies on the use of MMS services. The specific interface between TASE.2 and the control centre application is a local issue and not a part of this standard. The next figure shows the relationship of TASE.2 protocol with the rest of the OSI stack.

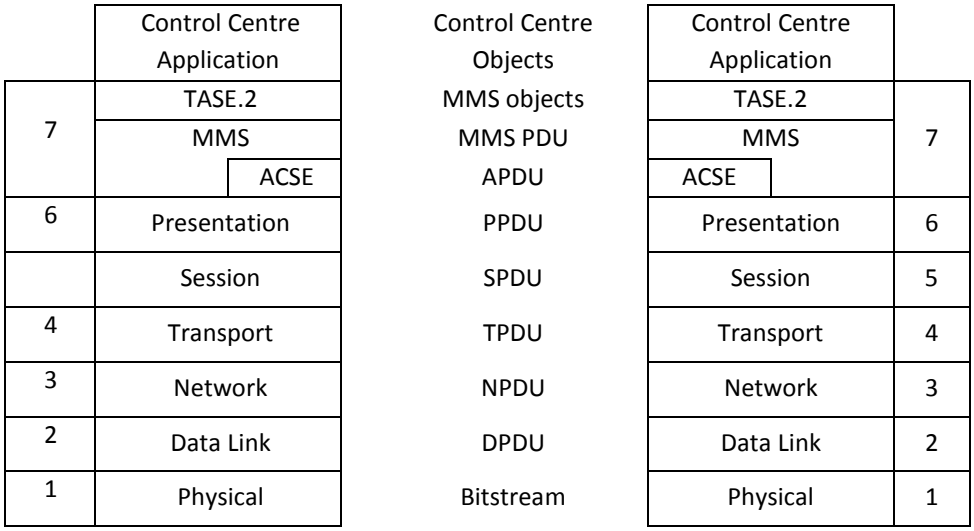


Figure 10.7 TASE.2 protocol relationships

The transport layers (1 to 4) can use any protocol, e.g. TCP/IP over any type of transmission media. The data exchange network can be either a private or public packet-switched or mesh network.

TASE.2 resides on top of MMS and enhances its functionality by specifying structured data mapped to MMS objects and assigning specific semantics to it. TASE.2 provides appropriate services not included in MMS by defining several conformance building blocks. MMS provides its services to TASE.2, and TASE.2 provides its services to the control centre application. In addition, MMS can provide services to users other than TASE.2.

In interactions with other computing elements, a control centre may act as a client, server or both. TASE.2 specification defines a number of operations and actions. Each operation begins with a local TASE.2 instance, acting as client, invoking a MMS service. A TASE.2 action begins with a local TASE.2 instance, acting as server, invoking an MMS unconfirmed service. Both actions and operations cause the local MMS provider to make use of the MMS protocol to communicate with remote MMS server. TASE.2 defines algorithms for both the client and server for each TASE.2 operation and action:

- **Relevant access control mechanisms**: they are implemented through bilateral agreements represented by a bilateral table. Every device object visible via TASE.2 shall be included in the bilateral table along with its access control specification.
- **Mapping between TASE.2 objects and MMS objects**.
- **MMS services and indications used**.
- **Relationship to real control centre functions**.

Data value objects are used to represent the values of control centre data objects. They may be any control elements, including points (analogue, digital, control) or data structures. There are four operations defined:

- Get data value.
- Set data value.
- Get data value names.
- Get data value type

Data Set objects are ordered list of data value object identifiers maintained by a TASE.2 server. Six operations are defined for manipulating Data Sets objects:

- Create data set.
- Delete data set.
- Get data set element values.
- Set data set element values.
- Get data set names.
- Get data set element names.

The protocol includes an **Information Message Object** for sending text or other data to an application at a remote control centre. It consists of a header and body. TASE.2 uses transfer set objects and services for exchanging data by reporting messages (text or binary).

Some TASE.2 objects, such as Data sets, a time series of a single data value and transfer accounts, may be transferred in a more complex scheme in which these objects are set up to be reported periodically, on change of object stated, or in response to particular server events. A critical data report mechanism has been also defined. A set of transmission parameters defines under what conditions data values shall be transmitted between server and client. For example, data set objects have conditions including interval timeout, value change, an integrity timeout, an operator request... The Transfer set operation defined are start transfer, stop transfer, get next transfer set value. Two TASE actions are also defined: condition monitoring and transfer report.

The following mechanisms are commonly used to exchange data between control centres (they are performed using one or more of the TASE.2 operations):

- **One shot data**: it is used to transfer data immediately. Typically a "get" operation associated with an object type (e.g. for an application such as the state estimator).
- **Periodic data**: set of control centre object values within a strict time interval.
- **Event data**: it is the same as the periodic data mechanism except that the data values are transferred under certain conditions: change of the status points, limit or dead band violation, data quality change, change in a tag value, operator request...

- **Exception data**: it is the same as the periodic data mechanism except that only the data values that changed since the last report are included.

There are **two classes of controllable devices** and the Device Object is used to represent both:

- **Direct control**: TASE.2 client operates on device objects at any time.
- **Select before operate**: TASE.2 must select the device object before operation. The server shall check if the device object is available and operable.

The operations for Device objects are the following: select, operate, get tag value and set tag value. The actions for these objects are timeout, local reset, success and failure. The following figure represents the device control sequence.

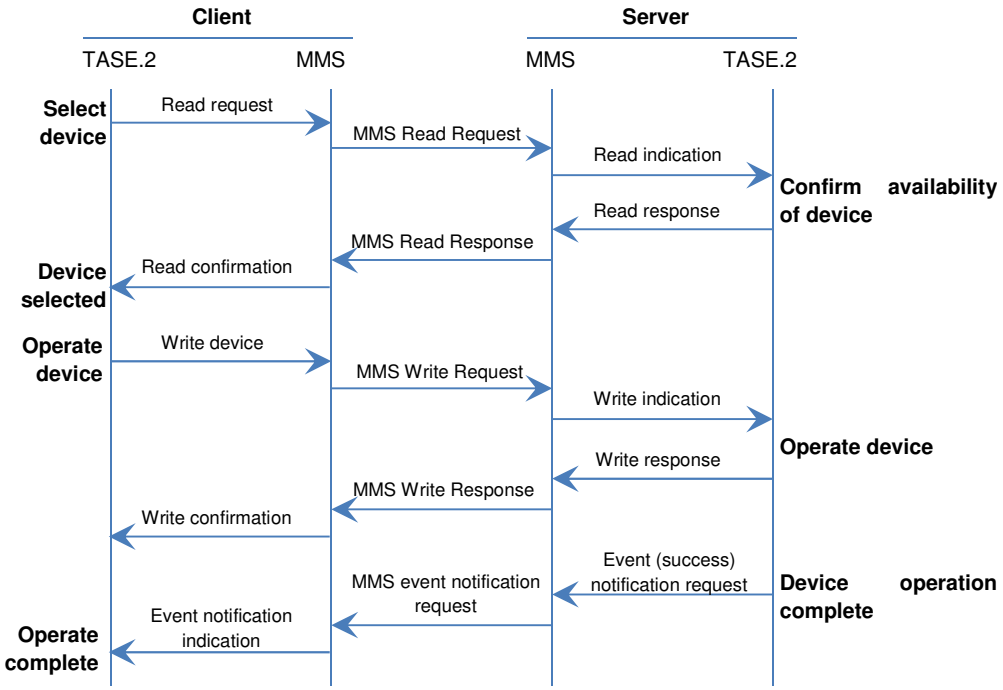


Figure 10.8 TASE.2 -sequence of device control

The following table gives a typical set of **application** priorities, nominal message lengths and desired response times offered in communications service.

Application message priority	Data	Priority Level (IP)	Nominal application data (Bytes)	Anticipated response (seconds)
1	System management	Reserved		1
2	Controls	High	100	1-2
3	Time Critical		50-500	1-10
4	Schedules	Normal	50 - 10kB	30
5	Critical text		8kB	30
6	Non-time critical	Low	kB	60
7	Non-critical text		8kB	60
8	Reports/information only	Low	unbounded	120
9	Long files		MB	300

Table 10.2 Typical communication service characteristics

10.5 IEC 61850

IEC 61850 is a set of standards originally developed for substation automation. It can be seen as a successor of IEC 60870-5 in some areas. It features a number of purpose-specific transmission options, and an object-oriented data model, as well as features where extensive tool-support can link in. Its application area has grown far beyond substation automation in recent years.

IEC – TC57 (Technical Committee) WG10 (Working group) is the group developing standards and technical reports related to the communication and data models of Power System IEDs. WG10 is also responsible for the generic aspects of IEC 61850 and coordinates with other WGs that are developing domain specific data models. The main scope is: Standards for 'Power system IEC communication and associated data models'.

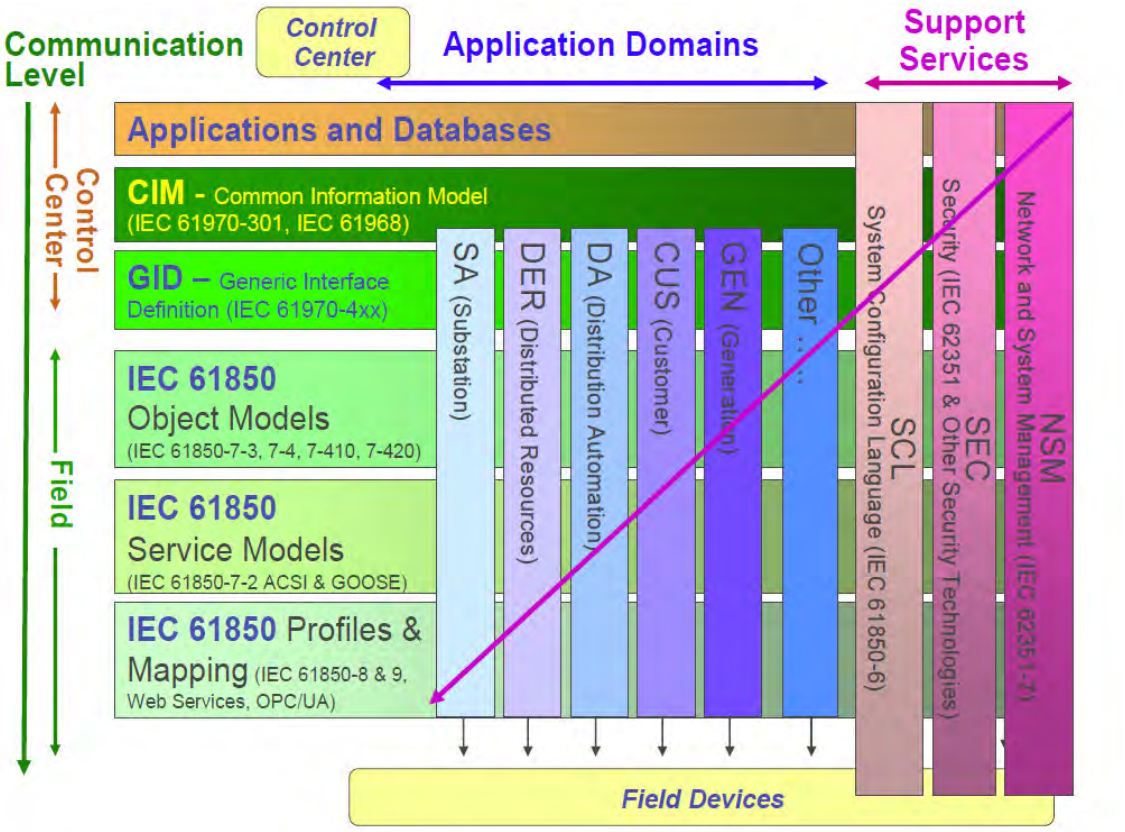


Figure 10.9 Interrelationship between IEC TC 57 modelling standards [41]

IEC 61850 consists of the following parts detailed in separate IEC 61850 standard documents:

- IEC 61850-1: Introduction and overview.
- IEC 61850-2: Glossary.
- IEC 61850-3: General requirements.
- IEC 61850-4: System and project management.
- IEC 61850-5: Communication requirements for functions and device models.
- IEC 61850-6: Configuration language for communication in electrical substations related to IEDs.
- IEC 61850-7: Basic communication structure for substation and feeder equipment.
    - IEC 61850-7-1: Principles and models.
    - IEC 61850-7-2: Abstract communication service interface (ACSI).
    - IEC 61850-7-3: Common Data Classes.
    - IEC 61850-7-4: Compatible logical node classes and data classes.
    - IEC 61850-7-410: Hydroelectric Power Plants - Communication for monitoring and control.
    - IEC 61850-7-420: Communications systems for Distributed Energy Resources (DER).

- IEC 61850-8: Specific communication service mapping (SCSM).
    - IEC 61850-8-1: Mappings to MMS (ISO/IEC9506-1 and ISO/IEC 9506-2).
- IEC 61850-9: Specific communication service mapping (SCSM).
    - IEC 61850-9-1: Sampled values over serial unidirectional multidrop point to point link.
    - IEC 61850-9-2: Sampled values over ISO/IEC 802-3.
- IEC 61850-10: Conformance testing.

The IEC 61850 originates from the domain of substations but its scope has been continuously extended, integrating various intelligent electronic devices (IEDs) in the energy distribution process. The standard defines a set of abstract objects and services virtualizing the state as well as functionality of IEDs.

Every **abstract model** of IED is composed of a set of Logical Devices and Logical Nodes, representing components and functionalities respectively. Each Logical Node refers to an Object Information Model (OIM), which defines a set of data objects and data attributes for the node. To communicate, Logical Nodes exchange information through an Abstract Communication Service Interface (ACSI). See the following figure.

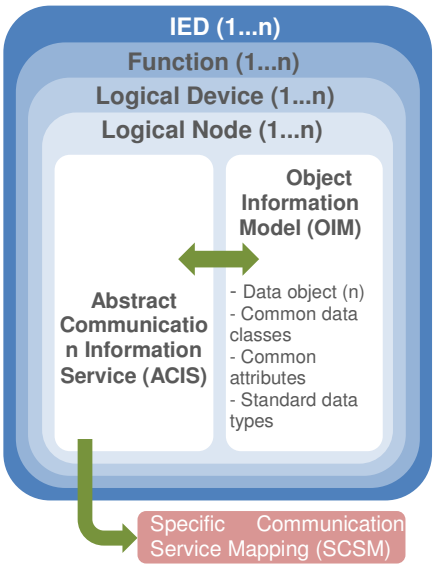


Figure 10.10 IEC 61850 Abstract model overview [42]

Any object within the data model can be referred to directly via its object path. An example is presented below:

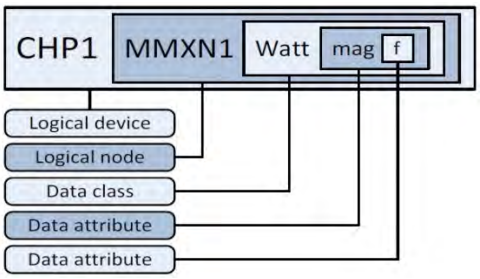


Figure 10.11 IEC 61850 Logical Devices and Logical Nodes overview [43]

IEC 61850 builds upon typical communication network protocol stacks like TCP/IP and/or Ethernet. It supports both client-server and peer-to-peer communication paradigms, typically used for less time critical communication services utilizing TCP/IP and real-time communication services using Ethernet (e.g. GOOSE, protocol for the distribution of event data), respectively.

In order to define the concrete interface to networking protocols and frame formats, the ACSI is extended by Specific Communication Service Mappings (SCSM). One SCSM example for the client-server based approach is the MMS.

		Application process	Information model (IEC 61850-7-4, IEC 61850-7-420)
			Abstract Communication Service Interface ACSI (IEC 61850-7-2)
		Specific Communication Service Mapping (SCSM)	
7	Application	MMS (ISO 9506)	
6	Presentation	ASN.1 ISI/IEC 8822	
5	Session	ISO/IEC 8326/8327	
4	Transport	TLS	
		TCP (RFC 1006)	
3	Network	IPv4 (RFC 791)	
2	Data Link	Ethernet (RFC 894), ISO/IEC 8802-2 LLC...	
1	Physical	Ethertype (ISO/IEC 8802.3)...	

Figure 10.12 IEC 61850 protocol stack for MMS based SCSM [42]

One of most important features of the IEC 61850 standard series is the object model. IEC 61850 is not just a protocol for transmission of data, but includes a complete description of all the objects that is exchanging information.

As illustrated in the figures, the object model is 'building blocks' called Logical Nodes (LN), ranging from measurements and DER types, to generation systems and management logical nodes. The object model in IEC 61850-7 includes the basic Logical Nodes to be used in substations and power systems, e.g. 'XCBR', which is the name for a LN used for modelling switches with short circuit breaking capability.

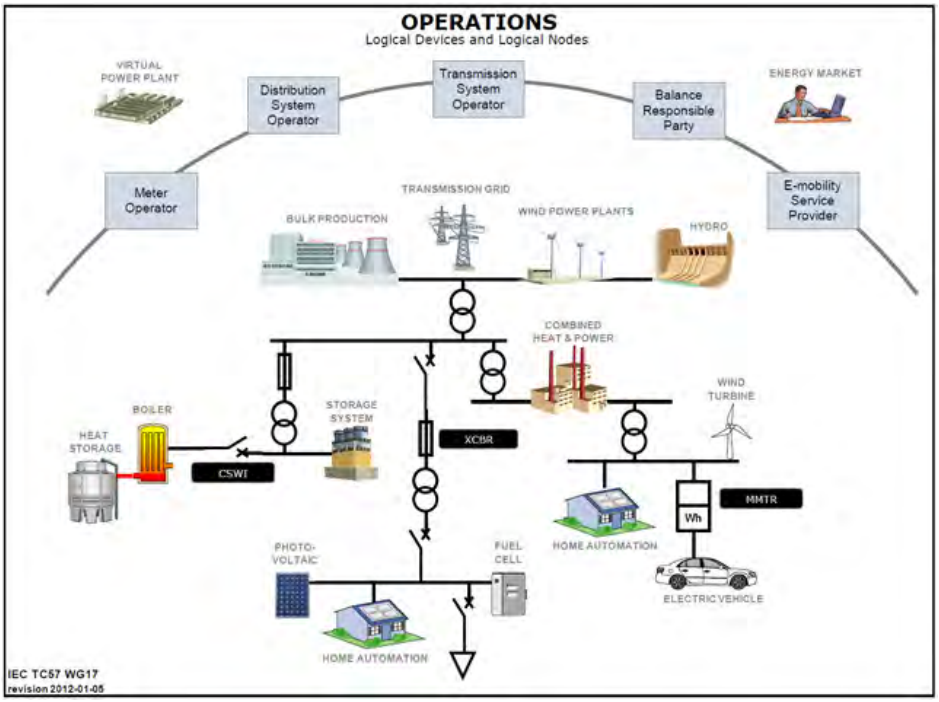


Figure 10.13 IEC 61850 Logical Devices and Logical Nodes overview (provided by EURISCO from IEC TC57 WG17 working document)

The IEC 61850 standard has evolved during the years with the extension for Distributed Energy Resources (DER), called IEC 61850-7-420. The next figure gives an overview of the DER Logical Nodes.

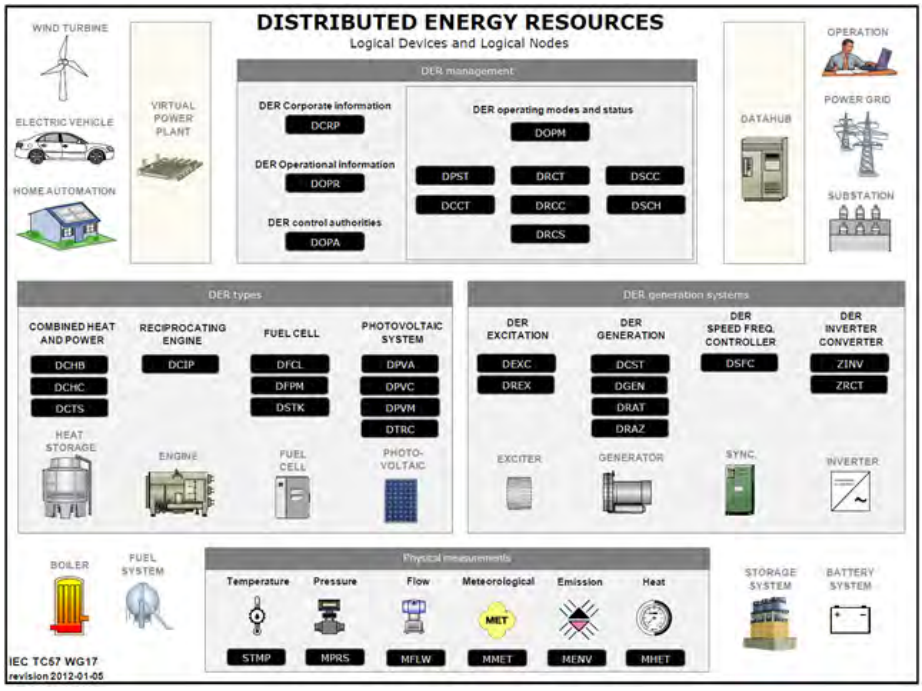


Figure 10.14 IEC 61850 DER Logical Devices and Logical Nodes (provided by EURISCO from IEC TC57 WG17 working document)

Also Photovoltaic (PV), Electrical Vehicle Supply Equipment (EVSE) and Battery Storage is going to be part of the coming next edition of the IEC 61850-7-420 standard (edition 2). Even if EVs are not yet considered in IEC 61850-7-420 as DER, an object model for electric mobility is published as IEC Technical Report 61850-90-8. The proposed object model satisfies the requirements of both ISO 15118 and IEC 61851-1 in terms of monitoring and parameterization of an EV charging process.

The 61850 standard also includes a protocol mapping called MMS (Manufacturing Message Specification) which originates from ISO 9506 and is called IEC 61850-8-1.

The MMS is a very effective binary mapping and a supplementary mapping based on XMPP/XML is under development with the name IEC 61850-8-2.

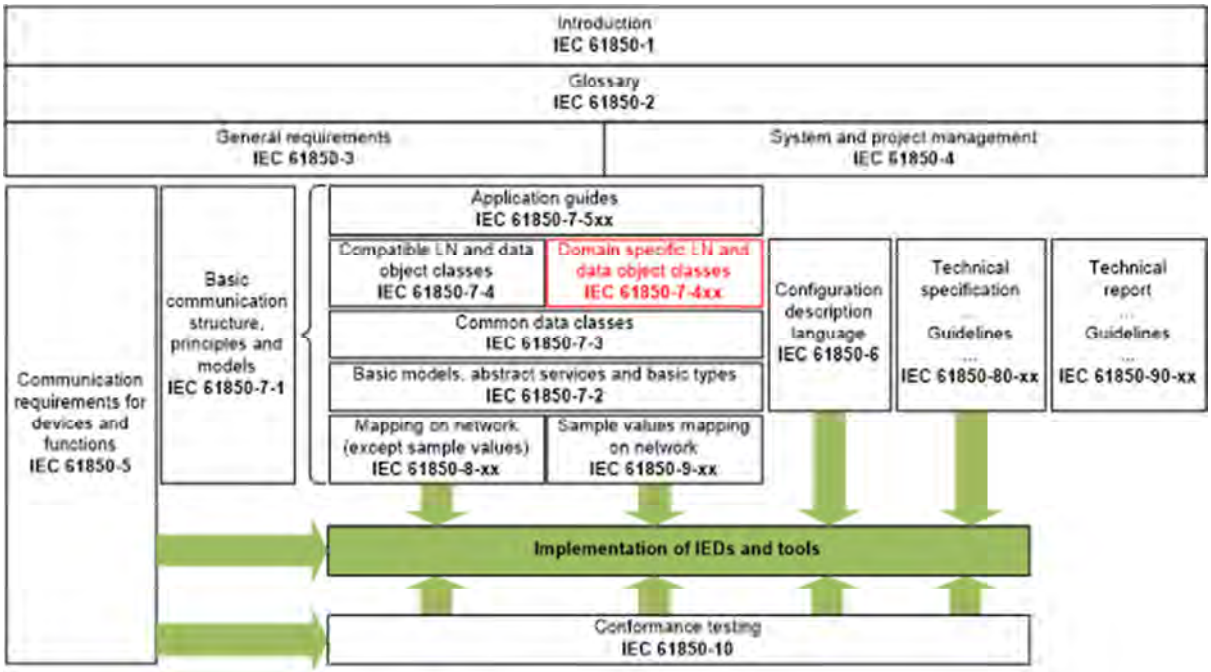


Figure 10.15 IEC 61850 parts and mapping[44]

According to [43], replacing MMS with REST services has certain advantages. REST services are a type of web services. While SOAP was embraced by most vendors and grew up via extensions, REST remains "lighter" and it is closer to the basic functionality of the HTTP protocol (get, post, put, and delete methods are used). The most important REST principle is to expose the resources in a RESTful service as unique URLs and the fact that IEC 61850 reference paths resemble a URL simplifies the task of creating a RESTful interface for the IEC 61850 data model.

The REST principles do not define any specific format for request or response data and, even if the XML is the most common, other such as JavaScript Object Notation (JSON) are becoming increasingly popular (especially in AJAX services).

The idea presented in [43] proposes that the various objects in the data model hierarchy can be thought of as resources, which can be accessed by using the IEC 61850 object reference. The ACSI

interface enables clients to inspect the data model, to read and write data and to access data-sets, logs, etc. To make a resource-oriented interface for the IEC 61850 standard, a mapping from the ACSI method to URL and HTTP method pairs was defined in [43]. Security could be addressed by using HTTP-basic authentication or X.509 client certificates.

10.6 IEC 61968

IEC 61968 is a series of standards for data exchange between electrical systems. These series define interfaces for the major elements of a distribution management architecture [45]. This International Standard series identify and establish recommendations for the standard interfaces based on an Interface Reference Model (IRM). These interfaces include:

- Part 1: Interface architecture and general requirements (common interfaces).
- Part 2: Glossary.
- Part 3: Interface for Network Operations.
- Part 4: Interfaces for Records and Asset management.
- Part 5: Interfaces for Operational planning & optimization.
- Part 6: Interfaces for Maintenance & Construction.
- Part 7: Interfaces for Network Extension Planning.
- Part 8: Interfaces for Customer Support.
- Part 9: Interface Standard for Meter Reading & Control.
- Part 10: Interfaces for Business functions external to distribution management.
    - Although this part was retired, it includes Energy management & trading, Retail, Supply Chain and Logistics, Customer Account Management, Financial and so on.
- It also contains series for Common Information Model (CIM).

To sum up, these set of standards are based on each interface identified in the IRM, providing interoperability among different computer systems, platforms, and languages. This way, it allows that utilities can integrate their systems and applications which need to collect data from different sources, regardless of their (old or new) technology, interfaces, languages or environments.

The IEC 61968 defines interfaces for all the major elements of an architecture for Distribution Management Systems and it is designed to integrate applications. This standard does not define the applications that vendors should implement, but the functionality that the concrete applications provide. This functionality is defined by one or more abstract components on the IRM.

The IEC 61968 series allows that applications can be loosely coupled by means of data exchange based on events. This way it is very easy to be integrated within message brokers middleware (e.g. Apache ActiveMQ™, JMS, MQ Series, etc.), message gateways and so on. It also defines the data model as XSDs, which allows an easy application integration by means of any well-defined protocol (Web Services,

RESTful). Moreover, companies which have been designed its systems as SOA (Service Oriented Architecture) can deploy the standard straightforward.

The standard is mature enough, providing a comprehensive data interchange, model and communications between systems.

The abstract components are grouped by the business functions of the IRM, containing not only the interface (function), but the data model for data exchange as well:

- **Network operation** (NO) business function:
  - Network operation **monitoring** (NMON): it provides the means for supervising the main substation topology and control equipment status, the utilities for handling network connectivity and loading conditions are also included, making possible to locate customer telephone complaints and supervise the location of the field crew.
  - Network **control** (NC): this sub-function is aimed for those decentralised control functions which have to be coordinated by an upper level system. It allows the automatic control using only local information without any knowledge of the network connectivity.
  - **Fault management** (FLT): it is intended to improve the speed of the fault detection and localization, as well as the service restoration.
  - **Operation feedback** (OFA): the data is retrieved from substation and customer records (registered) and compared with the real time data (network incidents, connectivity and loading).
  - **Operation statistics and reporting** (OST): for retrieving statistical on-line data and making reports, including feedback analysis of system efficiency and reliability.
  - **Network calculations** - real-time (CLC): this sub-function provides system operators with the ability to assess the reliability and security of the power system.
  - **Dispatcher training** (TRN): advanced function for training facilities for dispatchers, simulating the actual system that they will use to perform the dispatch function. This way, several scenarios can be tested.
- **Records and asset management** (AM) business function:
  - **Substation and network inventory** (EINV): functions for maintaining an accurate asset register hierarchically.
  - **Geographical inventory** (GINV): management of geospatial data, including graphic and non-graphic information.
  - **General inventory management** (GIM): an inventory for non-electrical assets that the utility owns, e.g. materials, vehicles and so on.
  - **Asset investment planning** (AIP): aimed for the planning, strategy definition and prioritization of assets.

- **Operational planning and optimization** (OP) business function:
  - **Network operation simulation** (SIM): functions for defining, preparing and optimizing the sequence of operations required for carrying out the maintenance work on the system and operational planning. The abstract components include load forecast, power flows computation, optimal power flow, weather forecast analysis, etc.
  - **Switch action scheduling / operation work scheduling** (SSC): support for handling all aspects relevant to switch order formulation, guidelines, dispatching repair crews and reports support for the affected customers.
  - **Power import scheduling and optimisation** (IMP): in order to minimize the cost of imported power by keeping the average imported power close to the contracted value.
- **Maintenance and construction** (MC) business function:
  - **Maintenance and inspection** (MAI): all work involving inspection, cleaning, adjustment and any other service of equipment for its optimal operation and extending its service life.
  - **Construction** (CON): for service installations, line extensions and system betterment projects.
  - **Design** (DGN): functions which allow engineers and work planners the design of components, such as construction engineering, cost estimation, bill of materials, etc.
  - **Work scheduling and dispatching** (SCHD): in a defined scope of work, functions to assign the required resources and keep track of work process.
  - **Field recording** (FRD): these functions are used by the field crew to view and enter information relevant to the work they are performing.
- **Network extension planning** (NE) business function:
  - **Network calculations** (NCLC): used to develop long-term plans for the reliability of the interconnected electric transmission and distribution networks.
  - **Construction supervision** (CSP): functions for monitoring and management of construction works to detect cost, performance or schedule deviations.
  - **Project definition** (PRJ): these functions enhance or extend the network and other assets, such as new substations, changing any component, etc.
- **Customer support** (CS) business function:
  - **Customer service** (CSRV): this sub-function covers the different aspects related to customers interfaces required for operation and commercial purposes.
  - **Trouble call management** (TCM): functions for troubles related to blackouts and any other incident.
  - **Point of sale** (POS): used for 'prepayment meters'.

- **Meter reading and control** (MR) business function:
  - **Meter reading** (RMR): this sub-function carries out remote readings of information recorded at the customer's point of supply, as well as those needed to send controls to customer equipment interfaces.
  - **Advanced metering infrastructure** (AMI): it includes advanced metering HW and SW to measure, collect and analyse energy usage and any other related information.
  - **Demand response** (DR): this sub-function manages customer consumption based on supply conditions and energy price.
  - **Load control** (LDC): customers who accept this option are able to adjust their consumption regarding Time of Use (ToU) tariffs. Automatic or manual equipment allows customers to adjust their consumption in response to the changes in the energy price.
  - **Meter operations** (MOP): functions for managing the deployment, maintenance and use of meters within a given service.
  - **Meter data management** (MDM): this sub-function collects, validates, stores and distributes readings and event related data from meters and any other end devices to other enterprise functions and systems. The MDM supports diverse end use applications such as billing, load management, load forecasting, demand response, outage management, asset management and distribution network planning and maintenance, but not limited to them.
  - **Metering system** (MS): for handling request and convey meter data, events, responses, system events and other value added data to the enterprise.
  - **Meter maintenance** (MM).
  - **Meter data** (MD): the meter records the data used for tariffs of public networks, data used for network balance mechanism and energy billing. Readings captured by meters are therefore integrated over a period of time before being sent for billing purposes. This way, billing entities may correct the data and validate it. The primary data used depends on the meter, such as active and reactive power indices, load curve schedule, current limitations, energy consumption, etc.
  - **Premise Area Network** (PAN).
- **External to DMS** (EXT) business function: this business function includes several sub-functions external to the distribution management system. This includes energy trading, retail, sales, stakeholder planning and management, supply chain and logistics, customer account management, financial functions, business planning and reporting, premises, human resources, public information, energy service provider (Aggregator), premise area network so far.

10.7 IEC 61970

The principal objective of the IEC 61970 series of standards is to produce standards which facilitate the integration of Energy Management System (EMS) applications developed independently by different vendors, between entire EMS systems developed independently or between an EMS system and other systems concerned with different aspects of power system operations, such as generation or distribution management systems. This is accomplished by defining application program interfaces to enable these applications or systems access to public data and exchange information independent of how such information is represented internally.

The IEC 61970 standard series consists of the following parts:

Part	Title
IEC 61970-1	Energy management system application program interface (EMS-API) - Part 1: Guidelines and general requirements
IEC TS 61970-2	Energy management system application program interface (EMS-API) - Part 2: Glossary
IEC 61970-301	Energy management system application program interface (EMS-API) - Part 301: Common information model (CIM) base
IEC 61970-401	Energy management system application program interface (EMS-API) - Part 401: Component interface specification (CIS) framework
IEC 61970-402	Energy management system application program interface (EMS-API) - Part 402: Common services
IEC 61970-403	Energy management system application program interface (EMS-API) - Part 403: Generic data access
IEC 61970-404	Energy management system application program interface (EMS-API) - Part 404: High Speed Data Access (HSDA)
IEC 61970-405	Energy management system application program interface (EMS-API) - Part 405: Generic Eventing and Subscription (GES)
IEC 61970-407	Energy management system application program interface (EMS-API) - Part 407: Time Series Data Access (TSDA)
IEC 61970-453	Energy management system application program interface (EMS-API) - Part 453: CIM based graphics exchange
IEC 61970-501	Energy management system application program interface (EMS-API) - Part 501: Common Information Model Resource Description Framework (CIM RDF) schema
IEC 61970-405	Energy management system application program interface (EMS-API) - Part 405: Generic Eventing and Subscription (GES)

Table 10.3 IEC 61970 standard parts

As can be seen the IEC 61970 is a lengthy standard with many details. This section will primarily give an overview of the Common Information Model (CIM) base as specified in IEC 61970-301.

The CIM is an abstract model that represents all major objects needed to model the operational aspects of an electric utility enterprise. The model includes classes with different attributes for objects, and relations between these objects.

Due to the large number of classes, the **CIM** is grouped into the following **logical packages**:

- **Domain** that is a data dictionary of quantities and units that define data types for attributes that may be used by any class in any other package.
- **Core** that contains the core power system resource and conducting equipment entities shared by all applications, in addition to common collections of those entities.
- **Operational limits** that models a specification of limits associated with equipment and other operational entities.
- **Topology** that is an extension to the core package and gives the physical definition of how equipment is connected together.
- **Wires** that is an extension to the core and topology packages modelling the electrical characteristics of transmission and distribution networks.
- **Generation** is separated in two sub-packages **production** that describes various kinds of generators and **generation dynamics** that contain prime movers, which are needed for simulation and educational purposes.
- **Load model** that models the energy consumers and the system load as curves including special circumstances such as seasons and day types.
- **Outage** that is an extension to core and wire packages that models information on the current and planned network configuration.
- **Protection** that is an extension to core and wire packages that model information for protection equipment such as relays.
- **Equivalents** that models equivalent networks.
- **Meas** that contains entities that describe dynamic measurement data exchanged between applications.
- **SCADA** that contains entities to model information used by SCADA applications, such as supervisory control and data acquisition of telemetered data. The defined types match those of IEC 61850.
- **Control area** that models area specifications used for a variety of purposes.
- **Contingency** that contains contingencies to be studied.

The CIM is given in UML and can be mapped to object-oriented programming languages. One example representation format is the Resource Description Framework (RDF) schema in XML that allows the description of a power system model to be shared among different implementations.

10.8 IEC 62056

IEC 62056 is a set of standards for Electricity metering data exchange and they are the International Standard versions of the **DLMS/COSEM** specification [46].

COSEM (Companion Specification for Energy Metering), includes a set of specifications that defines the transport and application layers of the DLMS (Device Language Message Specification) protocol. The DLMS User Association (UA) defines the protocols into a set of four specification documents namely Green Book, Yellow Book, Blue Book and White Book. The Blue Book describes the COSEM meter object model and the Object Identification System (OBIS) object identification system, the Green Book describes the architecture and protocols, the Yellow Book treats all the questions concerning conformance testing, the White Book contains the glossary of terms. If a product passes the Conformance Test specified in the Yellow Book, then a certification of DLMS/COSEM compliance is issued by the DLMS UA.

The IEC TC13 WG 14 groups the DLMS specifications under the common heading: "Electricity metering data exchange - The DLMS/COSEM suite". DLMS/COSEM protocol is not specific to electricity metering, but it is also used for gas, water and heat metering.

- IEC 62056-1-0:2014 Smart metering standardisation framework.
- IEC 62056-3-1:2013 Use of local area networks on twisted pair with carrier signalling.
- IEC 62056-5-3:2013 DLMS/COSEM application layer.
- IEC 62056-6-1:2013 Object Identification System.
- IEC 62056-6-2:2013 COSEM interface classes.
- IEC 62056-7-6:2013 The 3-layer, connection-oriented HDLC based communication profile.
- IEC 62056-8-3:2013 Communication profile for PLC S-FSK neighbourhood networks.
- IEC 62056-9-7:2013 Communication profile for TCP-UDP/IP networks.

Other IEC 62056 parts deal with Electricity metering - Data exchange for meter reading, tariff and load control:

- IEC 62056-21:2002 Direct local data exchange.
- IEC TS 62056-41:1998 Data exchange using wide area networks: Public switched telephone network (PSTN) with LINK+ protocol.
- IEC 62056-42:2002 Physical layer services and procedures for connection-oriented asynchronous data exchange.
- IEC 62056-46:2002+AMD1:2006 Data link layer using HDLC protocol.
- IEC 62056-47:2006 COSEM transport layers for IPv4 networks.
- IEC TS 62056-51:1998 Application layer protocols.
- IEC TS 62056-52:1998 Communication protocols management DLMS server.

The objects are modelled considering a three hierarchical level structure:

- **Physical device**: the meter is the physical device. It can support one or more communication profiles. Currently, the Standard specifies two profiles: the 3-layer, connection oriented HDLC-based profile (physical, HLDC and application), and the TCP-UDP/IP based profile. The device has a physical address that depends upon the supported profiles.
- **Logical device**: A physical device hosts one or several Logical Devices. A logical device models a specific functionality of the physical device. For example, in a multi-energy meter, one logical device could be an electricity meter, another, a gas-meter, etc. Each logical device has an address, called the logical device address. According to the standard, all physical devices have to host a special logical device called the management logical device, with the predefined address 1. The management logical device itself may contain a lot of information, but, at least, it has to contain a description of all the logical devices available in the physical meter, with their logical addresses and names.
- **Accessible COSEM Object**: a logical device is a container for COSEM objects. A COSEM object is a structured piece of information with attributes and methods. The first attribute of each object is its Logical Name. All objects that share the same structure are of the same COSEM class, which can be classified into four categories [47]:
    - **Data management**: demand register, profile register, status register, etc.
    - **Metering device configuration**: clock, activity calendar for Time of Use management, special days table, single action, schedule, disconnect control, etc.
    - **Interface classes for DLMS/COSEM communication management**: Service Access Point (SAP) assignment, application association and security setup.
    - **Interface classes for lower layer communication management**: each lower layer profile has a set of interface classes (direct communication, CSD, TCP-UDP/IP, PRIME, G3, GPRS...)

A logical name consists of a string of 6 values defined according to a system called OBIS (Object Identification System). OBIS allows to uniquely identify each of the many data items used in the energy metering equipment. The list of all possible OBIS codes (OBIS code is another name for logical name) is published by the DLMS Users. For instance the OBIS codes for ''active power'' and ''time integral'' are 1.1.1.8.0.255.

Several mandatory elements allow **getting the necessary information** about the content of a physical device:

- Each physical device has a management logical device, at address 1.
- A management logical device hosts a list of all the available logical devices in the physical device. This list is the second attribute of the object of class SAP Assignment, with the predefined name 0.0.41.0.0.255. Each list item consists of the name and the address of a logical device.

- Each logical device hosts a list of all its available objects. This list is the second attribute of the object of class Association, with the predefined name 0.0.40.0.0.255. Each list item consists (among others) of the logical name and the class of an object.

The data exchange between the data retrieval program and the meter uses the client-server model. The application is the client and the meter plays the role of server. The client sends requests (e.g. read an object at an address) and the server answers responses.

In the COSEM/DLMS communication framework, each side of the connection has an address. By definition, the client address is a byte value. Furthermore, the value of the client address determines also the real nature of the client. The standard states that a client with address 16 (decimal) is a public client.

There are several mechanisms to control the access rights. The simplest one is based on authentication and authorization. The meter recognizes the client address and presents (via the Association object) the objects allowed to be read or written.

10.9 IEC 62325

IEC 62325 represents a set of standards describing a framework for energy market communications. Its main parts are covering the communication between market participants and market operators. Two market styles are supported: European and US-style markets.

The principal objective of the IEC 62325 series is to produce standards which facilitate the **integration of market application software**, developed independently by different vendors into a market management system, between market management systems and market participant systems. This is accomplished by defining message exchanges to enable these applications or systems access to public data and exchange information independently of how such information is represented internally. The common information model (CIM) specifies the basis for the semantics for this message exchange [9].

The common information model is an abstract model representing objects, which are represented as public classes, including attributes for these objects and the relationship between them. As the objects represented by CIM are abstract they can be used in several applications in market management systems.

The IEC CIM 62325 series of standards currently consists of the following international standards, whereas the first two are the foundation of the IEC 62325 series [48].

Standard	Title
IEC 62325-301	Framework for energy market communications – Common information model (CIM) Extensions for markets.
IEC 62325-450	Profile and context modelling rules.
IEC 62325-351	Framework for energy market communications – CIM European market model exchange profile.
IEC 62325-451-1	Framework for energy market communications – Acknowledgement business process and contextual model for CIM European market.
IEC 62325-451-2	Framework for energy market communications – Scheduling business process and contextual model for European market.
IEC 62325-451-3	Framework for energy market communications – Transmission capacity allocation business process (explicit or implicit auction) and contextual models for European market.
IEC 62325-451-4	Framework for energy market communications – Settlement and reconciliation business process, contextual and assembly models for European market.
IEC 62325-451-5	Framework for energy market communications – Problem statement and status request business processes, contextual and assembly models for European market.
IEC 62325-503	Framework for energy market communications – Market data exchanges guidelines for the IEC 62325-351 profile.
IEC 62325-504	Framework for energy market communications – Utilization of web services for electronic data interchanges on the European energy market for electricity.

Table 10.4 IEC 62325 standard parts

The different parts of the standard are described shortly below:

- **IEC 62325-301**: it specifies the CIM for energy market communications and consists of three packages, namely MarketsCommon, MarketOperation, and MarketManagement. These packages are used to create the necessary objects for energy markets, in particular for the US market on the one hand, and for European-style markets on the other hand [49].
- **IEC 62325-351**: it was developed for Europe's internal electricity market [50]. Within this standard the European-Style market profile (ESMP) is defined and provides core components for the usage in the IEC 62325-451-n standards. These deal with specific core business processes for European markets, e.g., scheduling, settlement, capacity allocation and nomination, acknowledgement, etc.
- **IEC 62325-450**: its purpose is to define how profiles from the CIM can be created, and to give a set of related rules for this task. Next figure shows how IEC 62325-450 can be positioned in the IEC 62325 modelling framework.

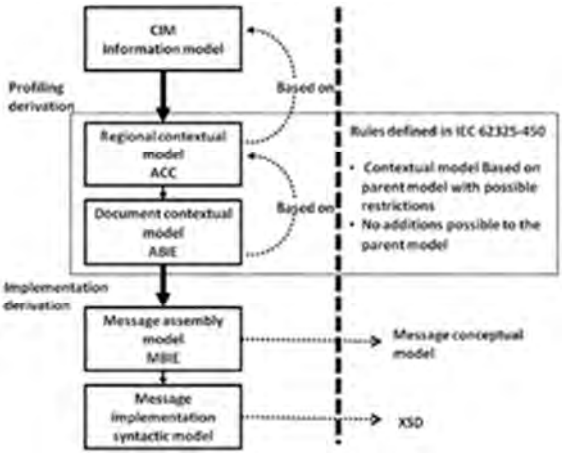


Figure 10.16 Modelling framework [50]

- **IEC 62325-451-1**: it specifies a UML package for the acknowledgment of business process and its associated document contextual model, assembly model, and XML schema for use within the European style electricity markets on the basis of Part 351. In IEC 62325-351, core components are defined, whereas in part 451-1 these elements have been contextualized into aggregated business information entities [51].
- **IEC 62325-451-2**: based on IEC 62325-351, this was developed to specify a UML package for the scheduling business process and its associated document contextual models, assembly models, and XML schemas for the usage within the European style electricity markets [52]. As in part 451-1 the components from IEC 62325-351 have been contextualized into aggregated business information entities.
- **IEC 62325-451-3**: it specifies a package for the transmission capacity allocation business process through explicit or implicit auctions and the associated document contextual models, assembly models, and XML schema for the usage in European style markets. It is based on the core components defined in IEC 62325-351 [53].
- **IEC 62325-451-4**: based on the core components of IEC 62325-351, this part specifies a package for the settlement and reconciliation business process and the associated document contextual model, assembly model, and XML schema for the usage within European style markets [54].
- **IEC 62325-451-5**: it specifies a package for the problem statement and status request business processes and the associated document contextual models, assembly models, and XML schema for the usage in European style markets. It is based on the IEC 62325-351 core components [55]. Next figure shows an overview of the European style market profiles dependencies as already described above.

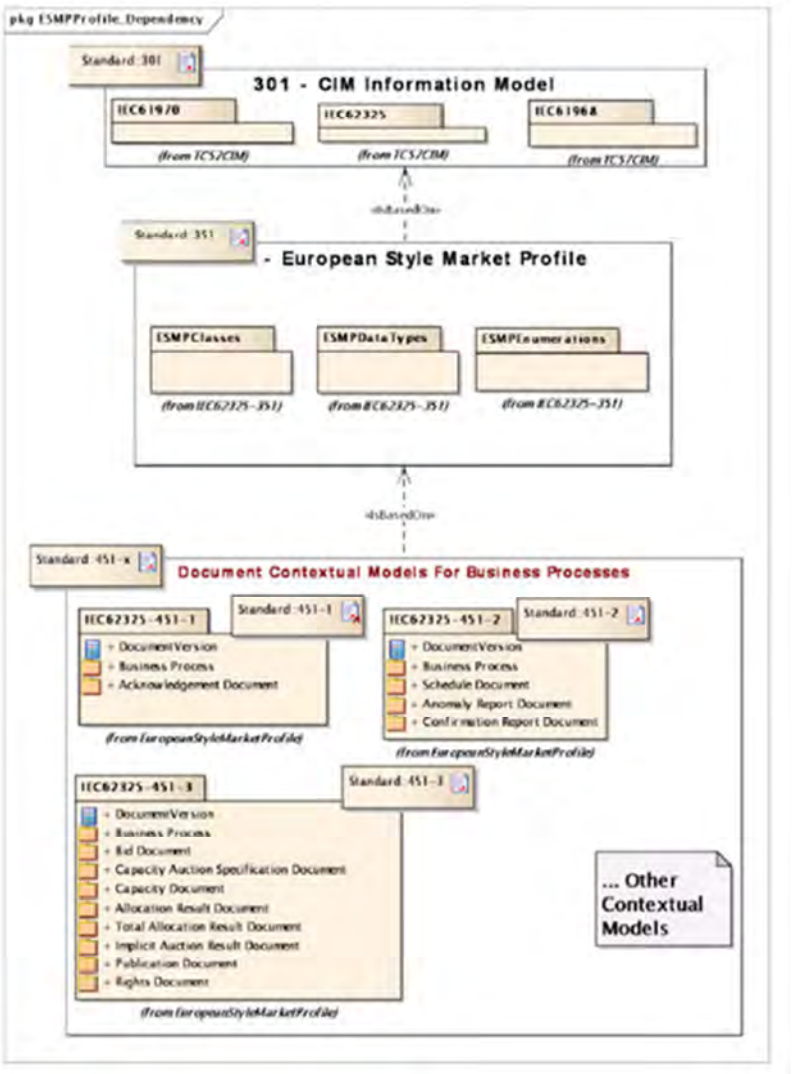


Figure 10.17 Overview of European style market profile dependency

- **IEC 62325-503**: the purpose of this technical specification is to provide guidelines to exchange the messages defined in IEC 62325-351 and IEC 62325-451-n. A European market participant (e.g., trader or distribution utilities) can benefit from a single, common, harmonized, and secure platform for message exchange with the European Transmission System Operators (TSOs). As a result, this would also reduce the cost of building different IT platforms to interface with all the parties involved. In addition, this also represents an important step in facilitating parties entering into markets other than their national ones [56].
- **IEC 62325-504**: this technical specification defines the services needed to support the electronic data interchanges defined in IEC 62325-401-n in a fast (near-real-time), and secure way. Web Services (in WSDL) are specified for the defined services, applying the Basic Web Service Pattern implementation profile from IEC 61968-100 [57].

10.10 IEC 62746 (Open ADR)

OpenADR is a communications data model, along with transport and security mechanisms, which facilitate information exchange between two end-points, the electricity service provider and the customer. OpenADR is designed to facilitate **Automated Demand Response** (ADR) actions at the customer location, including electric load shedding or shifting. OpenADR is also designed to provide continuous dynamic price signals such as hourly day-ahead or day-of real time pricing.

The Demand Response Research Center (DRRC) at Lawrence Berkeley National Laboratory (LBNL) developed the specification OpenADR 1.0 and donated it to the Organization of Structured Information Standards (OASIS) to create a national standard for OpenADR. The OASIS' Energy Interoperation (EI) Technical Committee (TC) developed the Energy Interoperation 1.0 standard. Considering that the goal of OASIS EI TC was more than DR and Distributed Energy Resources (DER), the EI TC created profiles within the EI Version 1.0 standard for specific applications within the Smart Grid. The OpenADR Alliance used the EI OpenADR profile as the basis for the OpenADR 2.0 Profile.

OpenADR 2.0 currently defines two **feature sets**, each of which represent a subset of OpenADR functionality. The feature sets are 2.0a, and 2.0b [58]. The purpose of these profiles is to create a range of functionality that can be supported by devices as simple as a thermostat (profile 2.0a) to more complex IT based systems such as might be used by aggregators (profile 2.0b).

There are two **types of nodes** in OpenADR communication exchanges: the Virtual Top Nodes (VTN) that publish information about upcoming events, and Virtual End Nodes (VEN) that receive these events, respond to them and eventually engage demand side resources. OpenADR nodes may communicate in either PUSH mode, where the VTN initiates application layer communication, or in a PULL mode, where the VEN requests information from the VTN to begin a series of message exchanges.

The standard defines the mechanisms for exchanging **application messages**, the messages exchanged, and the security mechanisms. Along with the specification the OpenADR Alliance created a separate subset schema XSD file containing each schema referenced by Energy Interoperation and used by OpenADR profiles.

OpenADR 2.0b makes use of standard-based IP transport mechanisms such as HTTP and XML Messaging and Presence Protocol (XMPP).

Two levels of **security** are defined for OpenADR 2.0, called 'Standard' and 'High'. The 'Standard' security uses TLS for establishing secure channels between a VTN and a VEN for communication. 'High' security additionally uses XML signatures providing non-repudiation for documentation purposes.

Considering the urgent need of industry that is starting to move ahead and cannot wait, the OpenADR 2.0b is published by the IEC as a Publicly Available Specification IEC PAS 62746-10-1:2014 [59]. It can temporarily be used as a reference, and gives time for IEC to develop a formal technical specification (TS)

or an international standard (IS) on Demand Response based on OpenADR 2.0b, fully compatible with IEC **CIM** which will then replace this IEC PAS.

The OpenADR profile specifications clearly define the expected behaviour when exchanging Demand Response (DR) event related information, however there is enough optionality in OpenADR that the deployment of VTNs and VENs is not a plug-n-play experience. OpenADR characteristics such as event signals, report formats, and targeting must be specified on a DR program-by-program basis. There is no such thing as a standardized DR program. Each DR program design tends to be unique, fitting the structural and regulatory requirements of the geographic region it is deployed in. For each DR program there are numerous possible deployment scenarios involving a variety of actors. The OpenADR 2.0 DR Program Guide provides a small set of clear recommendations that will address the majority of the details required to deploy a typical DR program, and to enable interoperability testing of equipment deployed in programs using the recommendations in this guide.

The guide contains templates for the **DR programs** shown below:

1. **Critical Peak Pricing**: rate and/or price structure designed to encourage reduced consumption during periods of high wholesale market prices or system contingencies by imposing a pre-specified high rate or price for a limited number of days or hours.
2. **Capacity Bidding Program**: a program which allows a demand resource in retail and wholesale markets to offer load reductions at a price, or to identify how much load it is willing to curtail at a specific price.
3. **Residential Thermostat Program/Direct Load Control**: a demand response activity by which the program sponsor remotely controls a customer's electrical equipment (e.g. air conditioner) on short notice. These programs are primarily offered to residential or small commercial customers.
4. **Fast DR Dispatch/Ancillary Services Program**: a demand response program that provides incentive payments to customers for load response during an Emergency Demand Response Event. An abnormal system condition (for example, system constraints and local capacity constraints) that requires automatic or immediate manual action to prevent or limit the failure of transmission facilities or generation supply that could adversely affect the reliability of the Bulk Electric System.
5. **Electric Vehicle (EV) DR Program**: a demand response activity by which the cost of charging electric vehicles is modified to cause consumers to shift consumption patterns.
6. **Distributed Energy Resources (DER) DR Program**: a demand response activity utilized to smooth the integration of distributed energy resources into the smart grid.

Commercial test suites are available to test for conformance to the OpenADR 2.0b Protocol Specification. A cloud based OpenADR VTN is available for test purposes. The OpenADR website lists

more than 100 commercial, certified OpenADR 2.0 products. Also several open source (reference) implementations are available for VTNs as well as for VENs. The OpenADR Alliance site provides a map with all (registered) OpenADR deployments.

In the European context, the OpenADR Alliance and the Universal Smart Energy Framework Foundation (USEF) recently signed a Memorandum of Understanding with USEF [60], a Dutch initiative, is a specification for flexibility trading developed by the USEF Foundation (ABB, Alliander, DNV GL, Essent, IBM, Stedin, ICT). The framework specifies the messages between different actors in the market.

The OpenADR 2.0b Feature Set was developed for advanced demand response systems and markets (e.g., wholesale and retail DR markets). It includes several services usable in Demand Response programs and for ancillary services. OpenADR 2.0b uses a profiled subset of the Energy Interoperation services tailored to meet the OpenADR needs, but conforming to the Energy Interoperation Specification.

The services supported by OpenADR 2.0b are:

- **The extended EiEvent Service**: this service contains the data model to issue demand response requests and is elaborated in more detail in the next paragraph.
- **EiReport Service**: OpenADR supports several report types. Each report type is intended to represent a certain set of reporting functionality that is supported by either a VEN or a VTN. The METADATA report is used to specify reporting capabilities. The DATA report is used to report actual data that may be measured or calculated. The core element of a Data Report is the so called “data point”. A data point represents a certain quantity that may be measured or calculated as part of a report. Each data point has attributes such as units, etc. A Data Report may contain one or more data points.
- **EiRegisterParty Service**: to support in-band registration of VENs with VTNs.
- **EiOpt service**: to create and communicate Opt-In and Opt-Out schedules from the VEN to the VTN. These schedules define temporary changes in the availability, and may be combined with longer term availability schedules and the Market Context requirements to give a complete picture of the willingness of the VEN to respond to EiEvents received by the VEN.
- **EiEvent Service**: events are generated by the VTN and sent to the VEN. Either a PUSH or PULL interaction pattern may be used. For push, the VTN will deliver events to the VEN. In PULL mode, events will be sent from the VTN to the VEN as response to a Poll request.

  oadrEvent elements describe individual events, signal values, and time periods (see next figure) that apply to signals. Each oadrEvent has an eiEvent element containing detailed event information.

  A single eiActivePeriod defines the start time and duration of the event. The start time is defined by an ISO 8601 time descriptor and an ISO 8601 duration string specifies the duration.

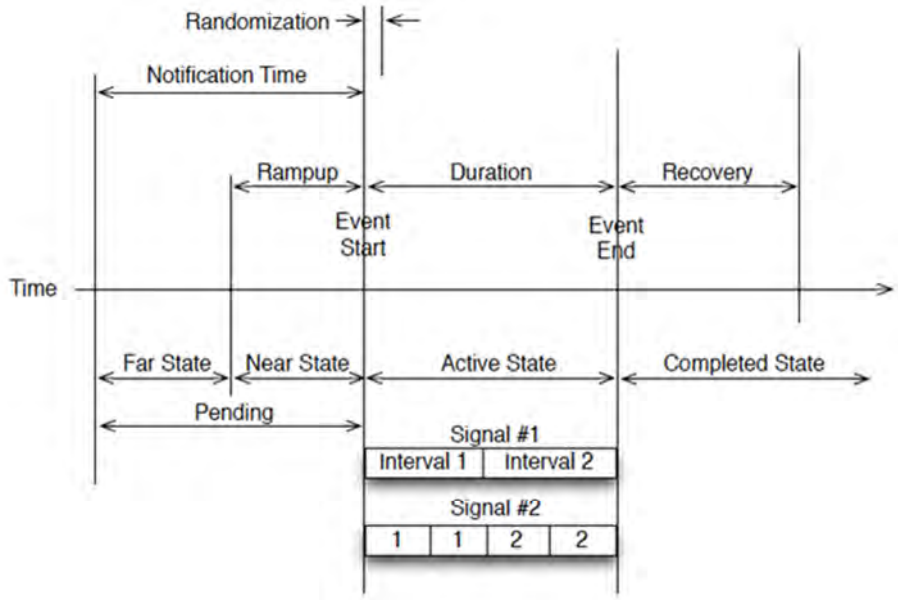


Figure 10.18 Time intervals of an event

The event signals that get applied over the entire active period are defined in an eiEventSignals element. This element contains one or more eiEventSignal elements, each with a sequence of durations, the sum of which must equal the full duration of the active period. Each signal element contains a signalType such as level or price. The signalPayload contains the value of the signal.

Several **signal categories** are available:

- **Simple level**: a DR signal in the context of an agreement-based interaction abstracted away from expressions of value or actual amounts.
- **Price of electricity**: a DR signal indicating the price of electricity expressed in absolute terms, relative terms or by a multiplier factor.
- **Price of energy**: a DR signal indicating the price of energy expressed in absolute terms, relative terms or by a multiplier factor.
- **Demand charge**: a DR signal indicating the demand charge expressed in absolute terms, relative terms or by a multiplier factor.
- **BID_ENERGY**: a DR signal indicating the amount of energy from a resource that was bid into a program.
- **BID_LOAL**: a DR signal indicating the amount of load that was bid by a resource into a program.
- **BID_PRICE**: a DR signal indicating the price that was bid by the resource.
- **CHARGE_STATE**: a DR signal indicating the requested state of energy storage resource in absolute terms, relative terms or by a multiplier factor.

- **LOAD_CONTROL**: a DR signal used to set load output to relative values.
- **LOAD_DISPATCH**: a DR signal used to dispatch loads to a specific amount, to some offset from an agreed upon baseline, as some multiple of power against some agreed upon baseline, or to a load expressed in terms of discrete levels.

Each signal is described by a **signal type**:

- **delta**: the signal indicates the amount to change from what one would have used without the signal.
- **level**: the signal indicates a program level.
- **multiplier**: the signal indicates a multiplier applied to the current rate of delivery or usage from what one would have used without the signal.
- **price**: indicates the price.
- **priceMultiplier**: the signal indicates the price multiplier. Extended price is the computed price value multiplied by the number of units.
- **priceRelative**: the signal indicates the relative price.
- **setpoint**: the signal indicates a target amount of units.
- **Load control signal types** to an instruction for the load controller to operate at:
    - x-loadControlCapacity: a level that is some percentage of its maximum load consumption capacity.
    - x-loadControlLevelOffset: a discrete integer level that is relative to normal operations.
    - x-loadControlPercentOffset: a percentage change from normal load control operations.
    - x-loadControlSetpoint: a load controller set point.

Specific deployments are free to define their own custom signals beyond what are defined above Additional mechanisms are provided in the standard to extend schema elements.

10.11 SEP 2.0

The Smart Energy Profile 2 (SEP 2.0) standard defines an application protocol to **enable utility management of the end user energy environment**, including concepts like demand response, load control, time of day pricing, management of distributed generation, electric vehicles, etc. In general, it serves two purposes:

- To inform the consumer (e.g. energy usage, pricing).
- To request actions to assist the grid (e.g. thermostat changes, PV inverter controls, plug-in electric vehicle charging).

The standard enables home energy information, control and management applications, as well as utility communications to devices in the home, via wired and wireless connections using the Internet Protocol.

The targeted deployment area for the protocol is the Home Area Network (HAN), but communication could be within a consumer home area network, to a consumer (energy management system or individual devices), or even to equipment directly connected to the distribution system such as Distributed Energy Resources (DER) and plug-in Electric Vehicles (EV).

The application protocol is built using the four-layer Internet stack model. It is designed to run over the Internet Protocol (IP) layer and is, therefore, media access control (MAC) and physical layer (PHY) agnostic. Depending on the physical layer (such as e.g. IEEE 802.15.4, power line communications, Ethernet or Wi-Fi) in use, a variety of lower layer protocols may be involved in providing a complete solution. The standard defines the mechanisms for exchanging application messages, the messages exchanged, and the security features used to protect the application messages. The following figure shows an example of Texas instrument ecosystems using SEP 2.0 [61].

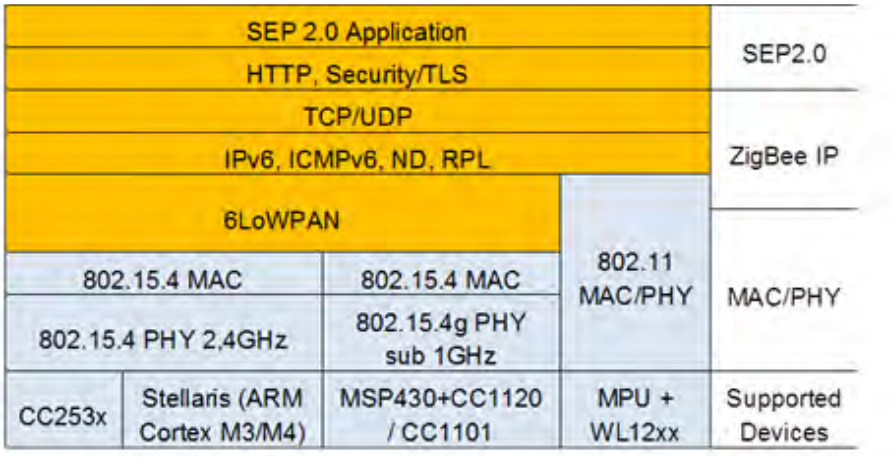


Figure 10.19 Example of Texas instrument SEP 2.0 application on top of a variety of lower layer protocols [61]

The standard follows an IETF RESTful (Representational State Transfer) architecture in which clients use HTTP methods GET, POST, PUT, and DELETE to engage with servers hosting resources. SEP 2.0 resources are identified and located by recommended URI structures. The distinction between a server and a client arises depending on whether a device exposes a resource (server) or interacts with the resource (client). Any device can be a server and/or a client. An HTTP (GET) method contains an XML or EXI payload. SEP 2.0 also provides an optional subscription mechanism that a client can use instead of polling the server for a resource using the HTTP GET method. This must be supported by the client and server devices and associated security protocols and firewalls.

The original work for SEP 2.0 was done via a joint liaison agreement between the ZigBee Alliance and the HomePlug Alliance and the resulting SEP 2.0 specification was published in April 2013. Control of future versions of the protocol was subsequently transferred to the IEEE and the April 2013 version of the standard was re-published as IEEE 2030.5:2013 (IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard). SEP 2.0 is described by its application standard, the associated SEP 2.0 XML Schema Definition (XSD) and SEP 2.0 Web Application Descriptive language (WADL). The Sep 2.0 specification is freely and publicly available [62].

Relation of SEP 2.0 with:

- **OpenADR**: this is a standard for demand response traditionally focused on commercial and industrial customers and on communication with entire premises. However, direct communication with end-devices at the customers' (also residential) premises is included in OpenADR 2.0. SEP 2.0, on the other hand, has traditionally focused on residential customers and on communication within the HAN. OpenADR 2.0 has a more focused scope, meaning demand response, than SEP 2.0. The two standards can work together quite well, for example, using OpenADR to communicate from the utility to an Energy Services Interface (ESI), and then using SEP 2.0 to communicate from the ESI into the home (see Figure 1).

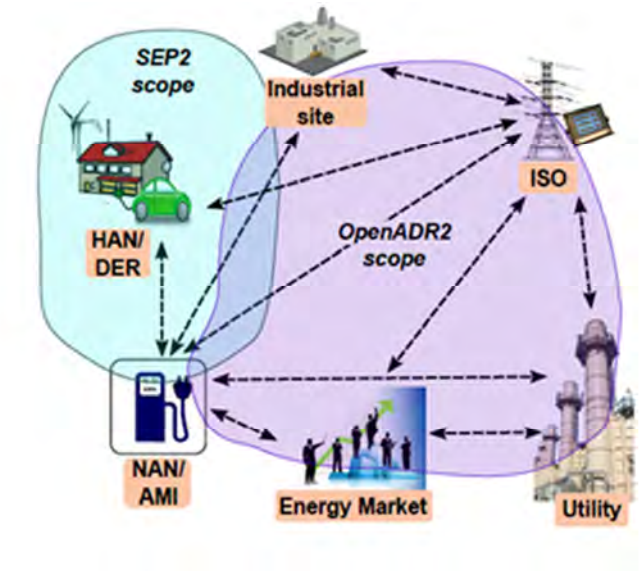


Figure 10.20 SEP 2.0 versus OpenADR 2.0 scope [63]

- **EEBus and SHIP**: EEBus [64] is a concept to develop interoperable Smart Home communication technologies based upon a neutral information layer with corresponding data models and their mapping onto different domain specific network technologies. The EEBus is the interface between the application layers of the different HBES/BACS/EMS (Home and Building Electronic System / Building Automation and Controls System/Energy Management System) protocols and the information from/to the Smart Grid. With this common interface,

the information exchange between these systems and the Smart Grid will be much easier and with a higher probability for interoperability between the different systems involved. The EEBus describes the information to the exchange, but there is no description or demand how to implement it.

SEP 2.0 can be one of the domain specific network technologies. For IP based communication the EEBus Initiative developed the SHIP (Smart Home IP) Protocol. It makes use of the EEBus data models, eliminating intermediate data model mappings. Therefore SEP 2.0 and SHIP may be very similar, targeting the same domains.

All EEBus specifications will become part of international Smart Grid and Smart Home standards (mainly IEC and CENELEC).

SEP 2.0 is selected by the United States National Institute of Standards and Technology (NIST) as a standard profile for smart energy management in home devices, and is a IEEE standard. The standard is based upon the IEC 61968 and IEC 61850 data models, two main smart grid data models, and uses common and mature ICT technologies.

To ensure interoperability of products, the members of the Consortium for SEP 2 Interoperability (CSEP) [65] are working together to develop common testing documents and processes for certifying SEP 2.0 interoperability. The consortium, initiated by HomePlug® Alliance, Wi-Fi Alliance® and ZigBee® Alliance, is focused on accelerating the market availability of interoperable Smart Energy Profile 2.0 products. Commercial test suites are available to test for conformance to the SEP 2.0 Application Protocol Specification.

In 2015 the California Public Utilities Commission and major utilities were working on plans to incorporate SEP 2.0 communications in DER integration projects. In parallel, South Korea is adopting SEP 2 for specific residential DR applications. Also several pilot projects on smart charging of electric vehicles are implementing SEP 2.0. It is not clear if and how many implementations of SEP 2.0 are currently in Europe. A quick scan resulted in a low number of commercial available products based upon SEP 2.0.

Before selecting a technology like SEP 2.0 one should investigate the use of EEBus/SHIP, which is not yet a standard, but a European initiative.

SEP 2.0 is an IEC 61968 **common information model** (CIM) profile, mapping directly where possible, and using subsets and extensions where needed. Where gaps existed, relevant information elements from IEC 61850 were included into the standard, for instance for DER modelling. The standard supports multiple commodities (electricity, water, gas, steam, etc.).

This standard addresses many functions (e.g. pricing communication, demand response and load control, usage information) and many types of devices (e.g., smart meters, thermostats, pool pumps, smart appliances, distributed energy resources, plug-in electric vehicles). The SEP 2.0 standard

functionality is organized into 23 function sets. All function sets do not have to be implemented in every device[11] and the requirements associated with a given function set may be mandatory or optional. Any device can be a server and/or a client for a function set: servers provide the data, clients use the data.

The **function sets** are divided into three areas:

- **Support resources**: these function sets provide operational information to the end devices of an SEP 2.0 network or provide those end devices with services to manage and support their operation. To these resources belong:
  - The **Device Capabilities Function Set**, enumerating the function sets supported by a device and to be used by clients to discover location information for the enumerated function sets.
  - The **Self Device Resource**, providing an interface for servers to publish general information about themselves.
  - The **End Device Resource**, providing interfaces to exchange information related to particular client device(s).
  - The **FunctionSetAssignments Resource**, defining collections of references to function set instances.
  - The **Subscription/Notification Mechanism**, supporting a generic, lightweight subscription / notification mechanism.
  - **The Response Function Set**, providing an interface for capturing responses from all events.
- **Common resources:** these function sets provide general purpose, non-domain specific functionality. These resources include:
  - The **Time Function Set**, to provide time synchronization of devices.
  - The **DeviceInformation Function Set**, to provide static manufacturer specific information about a device.
  - The **PowerStatus Resource**, to provide information regarding a device's current power source, as well as basic status regarding any battery installed within the device.
  - The **Network Status Function Set**, to provide information regarding the device's network (IP) layer, and potentially link layer, performance.

[11] An EV, for instance, may implement the following smart energy resources function sets: pricing, Demand Response and Load Control, metering, Distributed Energy Resource – Vehicle-to-Grid capability, as well as Flow Reservation function set.

- The **LogEvent List**, containing a list of time-stamped instances of LogEvents generated by the device.
- The **Configuration Resource**, implementing centralized read / write access to the device's operational configuration.
- **File Download Function Set**, to support secure, interoperable, remote software download to Smart Energy Profile 2.0 devices.

- **Smart energy resources**: these function sets are specific to the domain of Smart Energy. To these resources belong:
  - The **Demand Response and Load Control Function Set**, providing an interface for Demand Response and Load Control.
  - The **Metering Function Set**, providing interfaces to exchange commodity measurement information such as reading types and meter readings between HAN devices.
  - The **Pricing Function Set**, to provide the tariff structures communicated by the server. It is designed to support a variety of tariff types, including flat-rate pricing, Time-of-Use tiers, consumption blocks, hourly day-ahead pricing, real-time pricing, or any combination of the former mentioned tariff types. The Pricing Function set supports application-specific tariffs for devices (e.g. EV, DER), and special event-based prices like critical peak price.
  - The **Messaging Function Set**, providing an interface for a text messaging service.
  - The **Billing Function Set**, providing consumption or costs, estimates of future consumption, and / or historical consumption from a service provider to an end device.
  - The **Prepayment Function Set**, defining a mechanism for the conditional delivery of services based upon outstanding credit or debt.
  - The **Energy Flow Reservation Function Set**, providing an interface for exchange of energy flow (e.g., charge or discharge) reservation events. Client devices of this function set include plug-in EVs, distributed energy storage devices, and other managed loads that draw large amounts of power. Server devices of this function set include ESIs, EVSEs, and EMSs. FlowReservations allow for the scheduling of high demand periods such as during fast-charging transactions, to make them run at different times and avoid high aggregated demand.
  - The **Distributed Energy Resources Function Set**, providing an interface to manage Distributed Energy Resources (DER). Examples of client devices are fuel cells, intelligent solar inverters, backup generation units, battery storage systems and electric vehicles. Server devices of this function set include ESIs and premises energy

management systems. Servers host one or more DER Programs, which in turn expose DER Control events to DER clients.

- The **Metering Mirror Function Set**, providing a mechanism for constrained devices to post metering data to a metering server in a very efficient manner.

The standard provides also rules and mechanisms for third parties to extend the Smart Energy Profile 2.0 with proprietary extensions.

11 Appendix C: Security aspects and review of security standards

11.1 General aspects

ICTs are a core technology in smart grids and their deployment is expected to increase in the future. Because of this, the lack of security in ICTs would compromise energy system operation from two sides: reliability and data privacy.

In turn, security enhancement has direct impact on ICT features and design, both technically and economically. Processes such as encryption, signature inclusion, certificates handling, VPN tunnel building, etc. increase latency and volume of exchanged data, and require higher computational capabilities of the devices involved in them.

According to ENISA [66], the European Union Agency for Network and Information Security, cyber security should be considered in all domains of the smart grid and at all phases of the system life cycle. Security **threats** might be of different nature:

- **Deliberate or accidental:** safety failures, equipment failures, carelessness, natural disasters, etc.
- Caused by **people, processes, technology or external disasters.**
- **Technical:** malware, manipulation of devices, sensible information interception, denial of service, etc.
- **Organizational:** weak internal controls, procedures not followed, etc.
- **Information management:** low quality information for decision making, weak knowledge of regulations, etc.
- **Environmental:** natural catastrophe, nuclear catastrophe, pollution, etc.
- **Political:** war, terrorism, corruption, organized crime, etc.
- **Social and ethical aspects:** sabotage, error, panic, incompetence, dishonest behaviour, etc.

The **security level** asked to the different systems and applications of smart grids should depend on their criticality. A risk assessment helps define the main targets from security point of view. With the European electricity network in mind, the former European Commission DG INFSO's ad-hoc EG on cyber security aspects (currently DG Connect Trust & Security -H.4 unit-) suggested a two-step procedure for **risk assessment**: first, defining impact scenarios against which smart grids should be protected; and, second, classifying assets based on their criticality with respect to these scenarios:

- Assets that could cause an international cross border, national or regional power outage or damage to infrastructure.

- Assets that could cause a significant impact on energy market participants.
- Assets that could cause a significant impact on operations and maintenance processes on the energy grid.
- Assets posing a risk for data privacy of citizens.
- Assets causing significant safety issues for people.

In relation with this, the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) set up a team of experts to investigate the aspects related to Information Security (SGIS). During the first phase of M/490, Smart Grid Information Security Levels were defined (SGIS - SL) with the objective to create a bridge between electrical grid operations and information security, in order to increase grid resiliency [67]. These levels consider the fact that installed capacity at European level is more than 800 GW and that the loss of 10 GW may lead to a pan European incident (see Table 11.1).

Security level	Name	Expected power loss	Geographic impact
5	Highly critical	Above 10GW	Pan European
4	Critical	1 - 10GW	European/country
3	High	100MW - 1GW	Country/regional
2	Medium	1MW - 100MW	Regional/Town
1	Low	Under 1MW	Town/Neighbourhood

Table 11.1 SGIS security levels [67]

This European approach should be translated to other specific networks when dealing with them.

The Smart Grid Coordination Group developed the **SGIS toolbox** that describes a process for identifying the security criticality of information assets use cases within the SGAM framework [68]. However, the SGIS toolbox has not been adopted by the industry. The EU-funded SPARKS project has built on the experience from the SGIS toolbox and proposes a new methodology for risk management for smart grid ([68][69]).

The **SPARKS** process for **risk management** has four main topics as described in [69]:

1. **Context establishment**: defining the scope of the risk assessment to be carried out and the overall goals of the stakeholders involved.
2. **Impact assessment**: assessing the impact that incident scenarios will have to a target organisation, such as a DSO, energy supplier or other smart grid stakeholder; these impacts can be both cyber and physical in the context of the smart grid.
3. **Likelihood assessment**: determining the likelihood that an incident scenario will occur, based on a threat and vulnerability analysis.
4. **Security requirements and recommendations**: based on the assessed and evaluated risks, identifying set of security requirements and recommendations, typically drawn from best practice guidelines.

The risk management process from the SPARK project should be further evaluated and considered applied to the SmartNet project.

Once relevant assets and their criticality have been considered, the expected **causes of security flaws** must be studied to identify the specific requirements that will be asked to them. The following dimensions must be considered when managing ICT security [66][70]:

- **Integrity**: identifying and preventing data to be modified without authorization.
- **Availability**: identifying and assuring data and services that need to be available for a specific purpose at a precise time.
- **Confidentiality**: analysing whether some specific data should be protected from being accessed by unauthorized parties.
- **Authentication**: making sure that someone or something really is who or what claims to be, in order to ensure that the origin of the information is a valid originator and that it has the right to use a resource (authorization).
- **Non-repudiation**: proving that an action has been made by the entity responsible for that action, or even that a data signal or command has been provided or issued by the actual source.

Insufficient physical protection of infrastructures, insecure communication protocols, old equipment legacy, use of different security approaches, etc. can all be behind these security problems. Some general security measures for ICT systems are presented in the following table.

Functionality	Description
Encryption	All communication over public networks must be encrypted using proven encryption technologies. Communication over internal networks should be encrypted unless prohibited by reasons of efficiency and computational power.
Authentication	All actors connecting to the communication system must authenticate with a username/password or certificate.
Authorization	All access to information and services by actors in the system must be subjected to authorization rules. Unauthorized access must be prohibited. It should be possible to set authorization to create, update, access and delete operations separately.
Network separation	Communication networks in the operation zone and below should be separated from the enterprise network with a firewall, and only limited communication should be allowed through secure and controlled channels. An exception for this is the customer domain, where public wide area networks (i.e. the Internet) will be used for access between operation (such as aggregator) and station ("home box").

Table 11.2 General security measures for ICT systems

As mentioned above reliability of smart grid systems and processes, together with privacy issues, is another main risk area of poor ICT security. An increase of the reliability of the less reliable and/or more

critical components improves the reliability of the whole system. Below some typical strategies used to improve reliability related to ICT systems are presented [10]:

- **Hardware redundancy**: critical parts of the system are duplicated, e.g. power supply, data centre, control centre, communication mean, etc.
- **Data redundancy**: data is duplicated in more than one place within a computer system, e.g. by running two hard disks in parallel, disk mirroring.
- **Software redundancy**: more than one routine, written by independent coding teams, is produced. If there is no software failure all models produce the same output given the same input. If there is a disagreement a voting logic determines the operation.
- **Time redundancy**: performing the same operation multiple times, e.g. multiple copies of data transmitted.
- **Backing up**: the data is stored (duplicated) in separate locations, e.g. buildings, distributed clouds, etc.
- **Alternative paths for data transmission**: apart from hardware redundancy, meshed topologies permitting the dynamical selection of the best paths present better reliability levels.

11.2 Security from grid operator's point of view

The increased complexity of the electricity grid represents a challenge for network operators, since it involves a higher number of applications that depend on ICTs; an increased number of entry points and data paths; an increased amount of private information; and an increased use of new technologies, among others.

11.2.1Legacy Approach: Security by Obscurity

Communication protocols are one of the most critical parts of power system operations, both responsible for retrieving information from field equipment and, vice versa, for sending control commands. Despite their key function, to-date these communication protocols have rarely incorporated any security measures, including security against inadvertent errors, power system equipment malfunctions, communications equipment failures, or deliberate sabotage. Since these protocols were very specialized, “Security by Obscurity” has been the primary approach.

In addition to the national security concerns, **industrial espionage** threats are becoming more prevalent. The electricity market is pressuring market participants to gain any edge they can. A tiny amount of information can turn a losing bid into a winning bid – or withholding that information from your competitor can make their winning bid into a losing bid.

It is not only the malicious cyber threats that are making security crucial. The sheer complexity of operating a power system has increased over the years, making **equipment failures and operational mistakes** more likely and their impact greater in scope and cost. Natural disasters add to the need not just to prevent problems but to develop contingency plans and recovery measures. On the positive side, these same contingency plans can be used to mitigate malicious cyber-attacks.

11.2.2Smart Grid as Cyber-Physical Systems

Smart Grid systems are **cyber-physical systems**, which combine power system operational equipment with cyber-based control of that equipment. Cyber-physical systems are designed not only to provide the functions that the equipment was developed for, but also to protect that equipment against equipment failures and often against certain types of "mistakes". In addition, they are usually designed to operate in "degraded mode" if communications are lost or some other abnormal condition exists. "Coping" with attacks is also critical, since power system equipment cannot just be shut off if an attack is occurring, but must try to remain functional as much as possible. "Recovery" strategies after attacks are also critical, since again the power must remain on as much as feasible even if equipment is removed for repair. Finally, time-stamped forensic alarm and event logs need to capture as much information as possible about the attack sequences for both future protection and possible legal actions.

Therefore, cybersecurity for cyber-physical systems are mostly the same as for purely cyber systems, but there are some important differences. Cyber threats to the cyber-physical Smart Grid include:

- **Cyber impacts from physical attacks:** Physical attacks can harm the cyber controllers of power system equipment and communications networks. For instance, the theft of fiber optic cables or the disruption of wireless communications could cause denial of service that would prevent power system operators to manage the power system safely.
- **Impacts from cyber security:** Some types of cyber mitigation procedures and technologies can negatively impact cyber-physical systems. For example, if the time required to encrypt a message causes this message to arrive too late at the circuit breaker controller, that breaker might not trip in time. Therefore, the types of cyber security mitigations must be carefully woven into cyber-physical engineering mitigations to ensure that the primary functionality is maintained, even during attacks.

11.2.3Security for Profiles That Include TCP/IP

IEC 62351-3 [71] provides security for any profile that includes TCP/IP, including IEC 60870-6 TASE.2, IEC 61850 ACSI over TCP/IP, and IEC 60870-5-104.

Rather than re-inventing the wheel, it specifies the use of TLS which is commonly used over the Internet for secure interactions, covering authentication, confidentiality, and integrity.

Specifically, IEC 62351-3 protects against eavesdropping through TLS encryption, man-in-the-middle security risk through message authentication, spoofing through Security Certificates (Node Authentication), and replay, again through TLS encryption. However, TLS does not protect against denial of service. This security attack should be guarded against through implementation-specific measures.

11.2.4 Security for IEC 61850

The **IEC 61850** profile that includes the MMS protocol running over TCP/IP uses IEC 62351-3 and IEC 62351-4. Additional IEC 61850 profiles that run over TCP/IP (web services or other future profiles) will use IEC 62351-3 plus possible additional security measures developed by the communications industry for application-layer security (out-of-scope for this set of standards).

IEC 61850 contains three protocols that are peer-to-peer multicast datagrams on a substation LAN and are not routable. The main protocol, GOOSE, is designed for protective relaying where the messages need to be transmitted within 4 milliseconds peer-to-peer between intelligent controllers. Given these stringent performance requirements, encryption or other security measures which may significantly affect transmission rates are not acceptable. Therefore, authentication is the only security measure included as a requirement, so IEC 62351-6 provides a mechanism that involves minimal compute requirements for these profiles to digitally sign the messages.

11.3 X.509

The ITU-T X.500 series of directory standards dates back to the 1980, where the X.509 for **certificate based PKI** (Public Key Infrastructure) is a very important standard for information security in power systems [66].

This specification profiles the format and semantics of certificates and Certificate Revocation Lists (CRLs) for the Internet PKI. Procedures are described for processing of certification paths in the Internet environment. Finally, ASN.1 modules are provided in the appendices for all data structures defined or referenced.

Section 2 describes Internet PKI requirements and the assumptions that affect the scope of this document. Section 3 presents an architectural model and describes its relationship to previous IETF and ISO/IEC/ITU-T standards. In particular, this document's relationship with the IETF Privacy-Enhanced Electronic Mail (PEM) specifications and the ISO/IEC/ITU-T X.509 documents is described.

Section 4 profiles the X.509 version 3 certificate, and Section 5 profiles the X.509 version 2 CRL. The profiles include the identification of ISO/IEC/ITU-T and ANSI extensions that may be useful in the Internet PKI. The profiles are presented in the 1988 Abstract Syntax Notation One (ASN.1) rather than the 1997 ASN.1 syntax used in the most recent ISO/IEC/ITU-T standards.

Section 6 includes certification path validation procedures. These procedures are based upon the ISO/IEC/ITU-T definition. Implementations are REQUIRED to derive the same results but are not required to use the specified procedures.

11.4 ISO/IEC 27019 TR

The ISO/IEC 27107 is one of the "27000 series for securitization", based on ISO/IEC 27002 "Code of practice for information security management", which includes **information security management** applied to process control systems as used in the energy utility industry. The aim of this document is to extend the general ISO/IEC 27000 standards towards the domain of process control systems and automation technology, allowing the energy utility industry to implement a standardized Information Security Management System (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

As depicted in the next security standards coverage figure, this standard is focused on the details of operations, extending the general IT considerations. In other words, it covers **process control systems used by the energy utility industry** for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes the following **systems, applications and components**:

- The overall IT-supported central and distributed process control, monitoring and automation technology, as well as IT systems used for their operation, such as programming and parameterization devices.
- Digital controllers and automation components, such as control and field devices or PLCs.
- All additional supporting IT systems used in the process control domain (visualization, controlling, monitoring, data archiving, documentation...).
- The overall communications technology used in the process control domain, such as networks, telemetry, telecontrol applications and remote control technology.
- Digital metering and measurement devices (for measuring energy consumption, generation or emission values…).
- Digital protection and safety systems (protection relays or safety PLCs…).
- Distributed components of future smart grid environments.
- All related software, firmware and applications installed on above mentioned systems.

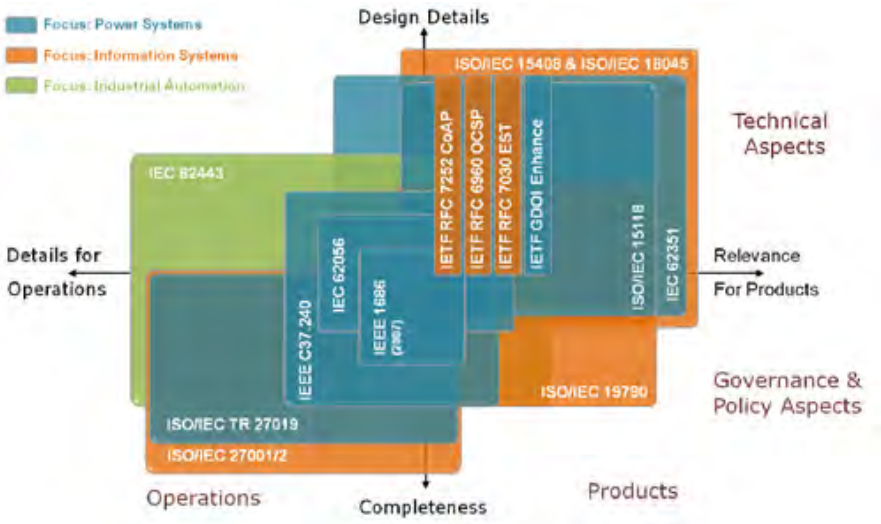


Figure 11.1 Security standard coverage. [5]

The pure electric and electromagnetic, as well as the telecommunication, systems are out of scope for ISO/IEC 27019.

The ISO/IEC 27019 defines the software and hardware components based on standard IT technology. Therefore, there are several options for implementing the security features defined in this standard. The first step for securing any system is to define up to what extend we want to secure our systems. The more security we want, the more technology and high processing equipment we need. Once the security level is defined, a complete set of procedures has to be applied to successfully comply with the requirements.

This standard provides the **guidelines for securing the data, assets**, physical and logical control access, security management, passwords, certificates, keys, revocations, signatures, etc. As a result, this security standard is complementary to other energy security standards, such as IEC 62351 which is focused on products/electric installations. This fact allows the seamless adoption of these technologies because it identifies the assets, the security we want to adopt and the security techniques that must be applied to all of them.

Anyway, some further considerations must be taken into account before establishing the **security level**. For example, if we wanted to avoid that an unauthorized person can connect to the communication network in an installation, we should detect that a person has entered into the perimeter, or that anybody is trying to insert or collect data from the communication channels or from the devices. Therefore, a complete policy must be available for describing this, in some installations the intrusion detection can be enough, whereas in others the user/password authorization must be implemented.

In order to establish the security policy, a comprehensive inventory of the resources must be available. In any energy system, diverse equipment is present with different computational and memory capabilities. The policy must gather which security (control access, signatures, encryption) is applied for

the devices. A device with little processing capabilities cannot execute the encryption algorithms, so its security policy differs from that of more 'intelligent' devices.

To sum up, the following steps can be observed before the implementation of this standard:

- A complete list of features for all devices and installations is needed.
- The capabilities per component have to be known and described.
- The policies for the installations, systems, devices and communications have to be established, taking into account the processing capabilities and the security level required.
- Devices must be interoperable: one device with high security level should be able to communicate with others with lower security levels.

11.4.1 Policy

The first step is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. This management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

The information security policy document should be published and communicated to all employees and relevant external parties. This document should state management commitment and set out the organization's approach to managing information security. It is a live document, so it should be reviewed at planned intervals or when a significant change occurs. This way, its effectiveness, suitability and adequacy is ensured.

11.4.2 Internal organization of information security

This feature manages the information security within the organization. Therefore, a management framework should be established according to the information security policy document, assigning roles and coordinating/reviewing the implementation of the security across the organization. It should support the security through a clear direction, commitment, explicit assignment and acknowledgment of information security responsibilities.

A management authorization process for new information processing facilities should also be defined and implemented. It includes management of personal laptops, which can introduce new vulnerabilities. Therefore the necessary controls should be identified and implemented too.

11.4.3 External parties

The objective is to maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties. It must ensure that the security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services. Therefore, any access to the

organization's information processing facilities and processing and communication of information by external parties should be controlled.

Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

11.4.4 Asset management

In order to achieve and maintain the appropriate protection of organizational assets, they should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

Once the inventory of assets and the owner identification have been defined, an information classification has to be done to ensure that information receives an appropriate level of protection. Therefore, the information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Notice that the information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

11.4.5 Human resources security

This feature is addressed to ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. The human resources security shall include the procedures for employees, including the existing staff, the applicants and the leaving crew. Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

It must be ensured that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support

organizational security policy in the course of their normal work, and to reduce the risk of human error. As a result, an adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to minimize possible security risks. Moreover, a formal disciplinary process for handling security breaches should be established.

When some entity (employee, contractor or third party) terminates the contract, it must be ensured that employees, contractors and third party users exit an organization or change employment in an orderly manner. This includes the return of all equipment and the access rights removal.

11.4.6Physical and environmental security

This feature secures areas (physical perimeters, entry controls, offices, rooms, facilities, control centres, as well as delivery areas, etc.), preventing unauthorized physical access, damage, and interference to the organization's premises and information. It also prevents loss, damage, theft or compromise of assets (equipment, cables, utilities, etc.) and interruption to the organization's activities. It also includes risks and protection against external and environmental threats.

A special mention is for the equipment located outside of the energy utility organizations' premises (third party or customer's premises), which has also to be protected against physical and environmental threats. Where energy utility organizations install equipment outside of their own sites or premises in areas that are the responsibility of other utilities, such as substations for instance, equipment should be sited in a protected area so that any risks arising from environmental threats or dangers are mitigated and the possibility of unauthorized access is reduced. The devices located in third parties' premises use to be interconnected with other third parties' components, so the responsibility and the interfaces between those components should be clearly defined.

11.4.7Communications and operations management

This feature ensures the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures. Moreover, segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

In the operating processes documentation, it should be specified exactly under which conditions incident, emergency or crisis handling procedures are to be invoked.

11.4.8Access control

This feature establishes that the access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. Access control rules should take account of policies for information dissemination and authorization. It also ensures

authorized user access and prevents unauthorized access to the information systems. Therefore, users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A weak point is the networks, so this feature must prevent unauthorized access to networked services, so both internal and external networked services should be controlled in order to user access to networks and network services should not compromise the security of the network services.

There are some other protections, such as operating system access control, mobile computing and teleworking.

11.4.9Information systems acquisition, development and maintenance

The security requirements of information systems are designed to ensure that security is an integral part of information systems. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services and user-developed applications. All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

This feature must also prevent errors, loss, unauthorized modification or misuse of information in applications, providing appropriate controls into applications which should include the validation of input data, internal processing and output data.

Cryptographic controls must be also applied to protect the confidentiality, authenticity or integrity of information by cryptographic means. A policy should be developed on the use of cryptographic controls. Moreover, a secure key management should be in place to support the use of cryptographic techniques.

There are other systems included in this features, such as:

- The security of system files to ensure the security of system files.
- Security in development and support processes to maintain the security of application system software and information.
- Technical Vulnerability Management to reduce risks resulting from exploitation of published technical vulnerabilities.

11.5 IEC 62351

The scope of IEC TC57 WG15 is to undertake the development of standards for **security of the communication protocols defined by the IEC TC57** [72].

TC57 WG15 is responsible for the IEC 62351 standards (some under development or update) consist of:

- IEC/TS 62351-1 Introduction.

- IEC/TS 62351-2 Glossary of Terms.
- IEC/TS 62351-3 Security for profiles including TCP/IP.
- IEC/TS 62351-4 Security for profiles including MMS.
- IEC/TS 62351-5 Security for IEC 60870-5 and derivatives.
- IEC/TS 62351-6 Security for IEC 61850 profiles.
- IEC/TS 62351-7 Objects for Network Management.
- IEC/TS 62351-8 Role-Based Access Control.
- IEC/TS 62351-9 Key Management.
- IEC/TS 62351-10 Security Architecture.
- IEC/TS 62351-11 Security for XML Files.
- IEC/TR 62351-12 Resilience and Security Recommendations for Power Systems with DER.
- IEC/TR 62351-13 Guidelines on What Security Topics Should Be Covered in Standards and Specifications.
- IEC/TR 62351-90-1 Guidelines for Using Part 8 Roles.
- IEC 62351-100-1 Conformance test cases for IEC 62351-5 and companion standards.
- IEC 62351-14 Security Event Logging and Reporting.
- IEC/TR 62351-90-2 Deep Packet Inspection.

There is not a one-to-one correlation between the IEC TC57 communication standards and the IEC 62351 security standards. This is because many of the communication standards rely on the same underlying standards at different layers. The interrelationships between the IEC TC57 standards and the IEC 62351 security standards are illustrated in the following figure.

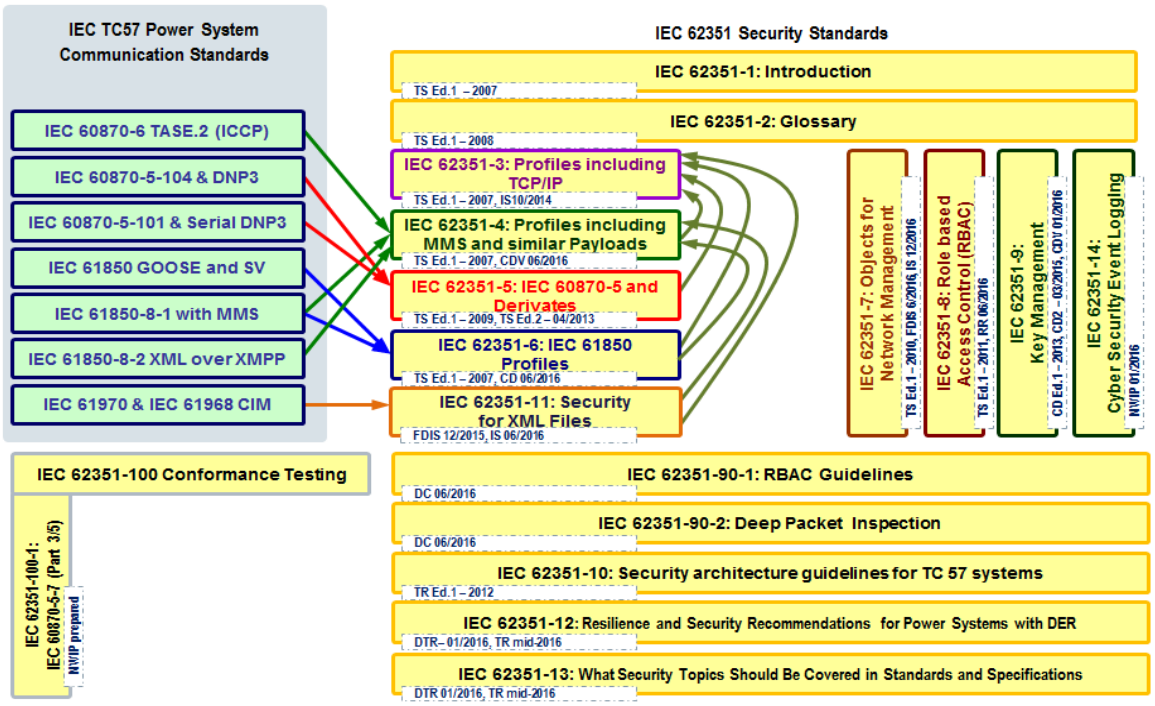


Figure 11.2 Relationship between IEC TC57standards and IEC 62351 security standard [73]

12 Appendix D: Smart grid components

The communication features of smart grid components determine, to a great extent, the remote control and monitoring functionalities of devices and systems. As a consequence, the characteristics of technologies and products available in the market have an impact on the design of network operation processes, including the use of flexibility resources.

Smart grid components cover most of the smart grid plane, as defined in the SGAM. In the following figure an overview of the main components (devices and systems) in smart grids is presented [5]. Normally, the communication links are established vertically in each domain or within each quadrant, but some interactions exist between them (see arrows in the figure as example).

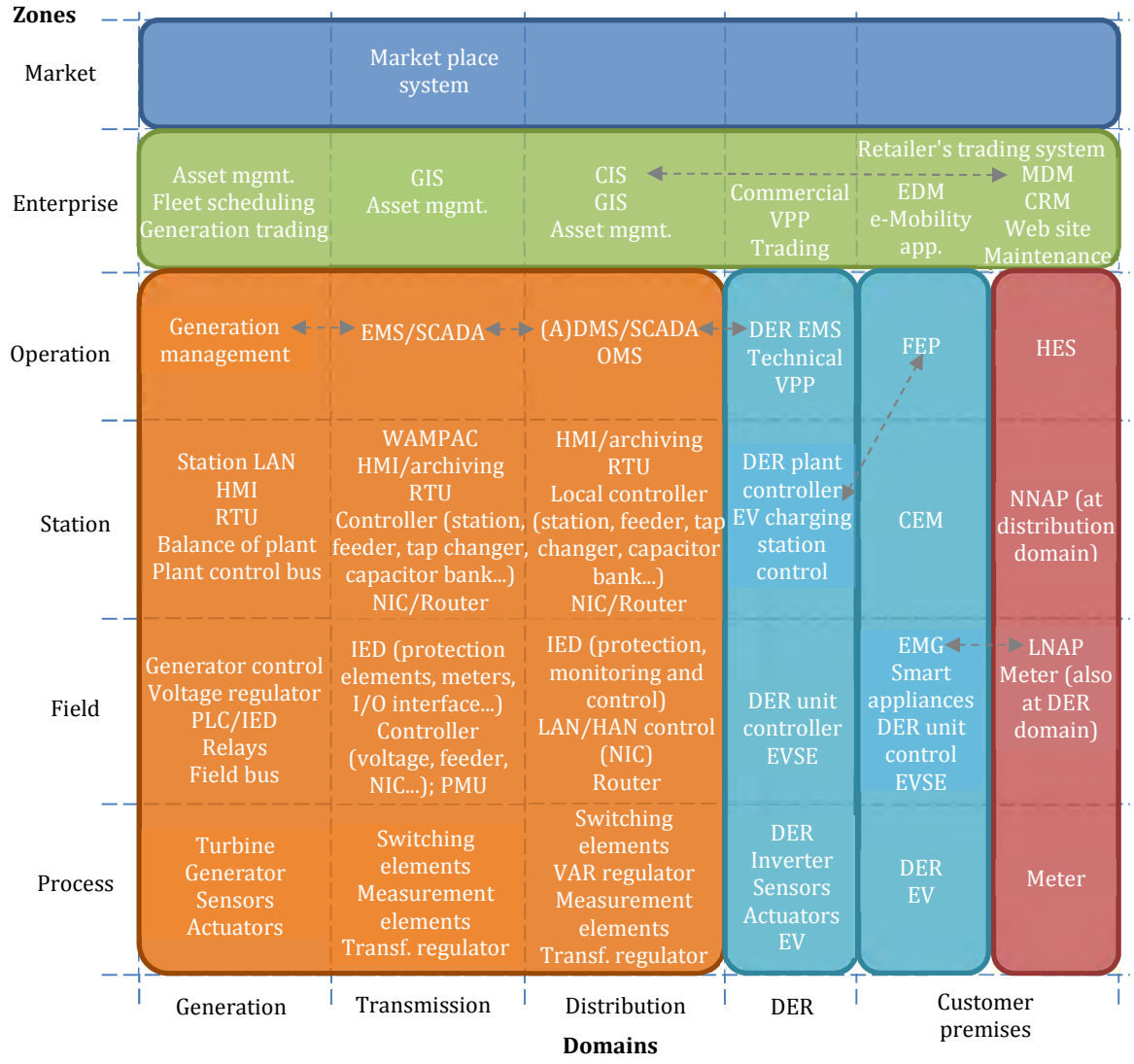


Figure 12.1 Overview of smart grid components mapped to SGAM

The components are classified here in five main fields:

- **Network operation** (in orange): it corresponds to components in the generation, transmission and distribution domains participating directly in network operation.
- **DER** (in light blue): systems participating in the operation of Distributed Energy Resources, which can be connected either to the distribution system or to customer premises. Within DER, various concepts are included: Distributed Generation (DG), storage, Demand Response (DR) and Electric Vehicles (EVs). The latter are explicitly mentioned in the figure because they require specific charging infrastructure.
- **Advanced Metering Infrastructure - AMI** (in red): infrastructure required for metering data retrieval. Metering infrastructure could also be used for load control (DR).
- **Enterprise processes** (in green): systems supporting commercial, organizational and, in general, not operational processes.
- **Market systems** (in dark blue): currently, market systems are managed by Transmission System Operators (TSOs) and by Independent Market Operators (IMOs). Distribution Systems Operators (DSOs) are not allowed to sell or buy services from them in most cases.

An overview of the main network components referenced in Figure 12.1 is presented below in accordance with the previous classification.

- **Network operation**:
    - **Software applications**: software backend applications have a crucial involvement in the generation and management of data for network operation processes. Common data formats, such as Common Information Model (CIM), provide better interoperability between applications and with the infrastructure, which improves efficiency and reduces costs.

      Operation level applications are in charge of controlling network infrastructures, DER systems and customer premises loads, generators and storage, depending on the business actor responsible for the management. In addition, they provide information to the applications in charge of the enterprise level processes. The main applications at network control centres are the following:

        - **Supervisory Control and Data Acquisition (SCADA) system**: general term describing the application used to control and monitor network infrastructure. It is related to the Energy Management System (EMS) of the TSO, the Distribution Management System (DMS) of the DSO and the DER EMS of the DER operator.
        - **Generation management**: application used to schedule bulk power generation plants, simulate their operation, etc.

        - **Outage Management System (OMS)**: application designed to help a network operator to handle outages in accordance to many criteria [5].
    - **Infrastructure:** network infrastructure is distributed through smart grid domains (from generation to customer premises connection point). The main **station level** components are linked to local substation control:
        - **Human Machine Interface (HMI) and archiving**: for local operators to visualize and archive local data.
        - **Remote Terminal Unit (RTU)**: microprocessor controlled electronic device that interfaces physical network components to a SCADA by transmitting telemetry data to the master system and control messages to end devices.
        - **Controllers (station level)**: station controller for automatic functions, feeder controller, capacitor bank controller, load tap changer controller, etc.
        - **Controllers (field level)**: feeder controller for connecting/disconnecting/reclosing sequences, voltage regulator controller, etc.
        - **Intelligent Electronic Device (IED)**: generic term covering components at field zone such as protection relays, meters, fault detectors, reclosers, bay controller, generic I/O interface and switch controller.
        - **Communications**: Network Interface Controller (NIC) and/or router connecting the LAN and WAN networks.
        - **Wide Area Monitoring system (WAMPAC)**: normally, at transmission level. It is the application that evaluates incoming data from Phasor Measurement Units (PMU) to derive information about the dynamic stability of the grid.
        - **Process level equipment**: primary equipment of substations, including switching, e.g., circuit breakers, switches and disconnectors; power transformer regulator; measuring elements, e.g., current and voltage sensors and transformers; Volt Ampere Reactive (VAR) regulators; FACTS; etc.
- **Distributed Energy Resources (DER) operation:** DER can be connected either at customer premises (home, commerce, industry) or directly to the distribution grid. The main components involved in the operation of DER are the following [5]:
    - **DER EMS**: control centre level management system to operate several DER plants, for instance, for a party owning different plants. It can be connected to the operators DMS.
    - **Technical Virtual Power Plant (tVVP)**: application to manage several DER plants as a virtual power plant based on technical criteria. It can be connected to the operators DMS.

- **DER plant controller**: station level controller, e.g., controller of a wind farm. In the case of a Charging Service Operator (CSO) this would be the EV charging station control system.
- **DER unit controller**: it is the controller of a DER unit, e.g. controller of a wind mill, EV supply equipment (EVSE), smart appliances controller, etc.
- **DER**: They include power generation and storage technologies plus demand response enabling strategies and devices, such as smart appliances and EVs. Systems include also inverters, sensors, actuators, etc.
- **Front End Processor (FEP)**: System component in charge of interfacing several spread remote components or subsystems, usually communicating over a Wide Area Network (WAN), to a central database [5]. Here, it is considered as part of the operation centre of the small size resource aggregator.
- **Customer Energy Management (CEM) system**: device for energy customers (home, industry, commerce) to optimize the utilization of energy according to supply contracts, demand response strategies or other economic targets. DER at customer sites could be managed from this type of system.
- **Energy regulation interface (ERI)**: it is a type of CEM system, which comprises several regulation and control functions of the customer generators and plant components. It can be implemented either directly on inverters or on specific equipment. It translates regulation requests to the commands and signals that are typical of the system that manages generators. It sends back measurement and state signals of plant equipment.
- **Energy Management Gateway (EMG)**: gateway used to interface the private area with remote service providers and with the smart metering system. To access DER in customer premises.

- **Advanced Metering Infrastructure (AMI) management:** The exact composition of the AMI depends on the configuration chosen, but the components that may be part of such system are the following [5]:
  - **Meter**: they represent end devices at process and field levels. It might be at customer premises (home, industry, commerce) or at DER domains.. Smart meters may have remote monitoring and load control capabilities, usually through the activation of relays. They might also be interfaced to a proper energy management system, such as a home automation system.
  - **Local Network Access Point (LNAP)**: they may be used to interconnect upstream AMI communication networks to meters and home/building automation.
  - **Neighbourhood Network Access Point (NNAP)**: typically at the station level of the distribution domain (relocated in Figure 12.1). It might be part of a data

concentrator, for instance, located at MV/LV substations, or a simple communication gateway.

- **Head End Systems (HES)**: Central data system exchanging data via the AMI of various meters and supervising the WAN/LAN communication. Meters can be connected to it either directly or via LNAP, or NNAP.

- **Enterprise processes:** Enterprise level processes are performed through applications that provide functionalities such as operation support, trading, finance/accounting, sales, billing, customer management, etc. Here below are listed the most typical ones [5]:
  - **Asset management**: it is common of all enterprises owning infrastructure. It is an application that optimizes the utilization of assets regarding loading, maintenance and lifetime.
  - **Customer Information System (CIS)**: it maintains all needed information about energy customers. It is normally associated with call centre software to provide customer services.
  - **Customer Relationship Management (CRM)**: it analyses customer data in order to retain them in the company through marketing, sales, support and feedback.
  - **Geographic Information System (GIS)**: it is an application designed to capture, store, manipulate, analyse, manage and present all types of geographical data. In the simplest terms, GIS is the merging of cartography, statistical analysis, and database technology.
  - **Trading systems**: they are used in all domains to interact with, normally, with a market place system. They permit to offer or purchase services, to settle agreements, etc.
  - **Commercial Virtual Power Plant (cVPP)**: application to manage several DER as a virtual power plant based on commercial criteria. It interacts with the market system or directly with an energy retailer.
  - **Energy Data Management (EDM)**: generic application permitting the management of customer energy data, for example, to a flexibility service supplier or an aggregator.
  - **Electro-Mobility (e-Mobility) application**: EDM specific for e-Mobility customers, i.e., valid for e-Mobility service providers.
  - **Meter Data Management (MDM)**: it is part of metering (AMI) related back-office system. It interfaces to market systems and to the Enterprise Resource Planning (ERP) systems (enterprise processes), such as CRM systems, maintenance management systems, etc. It may also interact with distribution network systems such as the DMS/SCADA or the GIS system. It receives metering tasks, such as data

acquisition and command distribution, communicates with AMI end points via the HES and returns the validated results.

- **Internet portal**: apart from CIS and CRM systems, today it is common the existence of consumer internet portals.

- **Market systems:** Energy markets operators (wholesale, ancillary services, forward capacity, etc.) have well-defined formats for exchanging information, normally, through a market system application accessible via internet (web services). Market place systems are accessed by market participants who can be electricity power producers, suppliers, industrial consumers, virtual power plants, aggregators, DER operators and similar, depending on the market rules.

13 Glossary

Access Point Name (APN): it is the name of a gateway between mobile networks and another computer network, frequently the public internet.

Enterprise Resource Planning (ERP) systems: they integrate internal and external management information across an entire organization, including finance/accounting, manufacturing, sales, customer relationship management, etc. [5]

Leased line: private line provided in a exchange of a monthly rent.

Multiprotocol Label Switching (MPLS): it is a type of data-carrying technique for high performance telecommunication networks using short path labels instead of long network addresses. It supports a range of access technologies and network protocols. The MPLS network connects the aggregation points with the last mile access points towards customer's infrastructure. By collecting more than one aggregation point or last mile access point, geographical redundancy can be provided.

Network Interface Controller (NIC): computer hardware component that connects a computer to a computer network. It works as bridge between a LAN and a WAN. Also known as network interface card, network adapter, LAN adapter...[5]

Node B: base station for UMTS mobile technology. eNodeB evolved base station for LTE.

Public Land Mobile Networks (PLMN): Network established by an administration or recognized operating agency to provide telecommunication services to the public.

Station controller: Automation system monitoring and controlling the devices in a substation. Provides interface to network control centre [5].

Supervisory Control and Data Acquisition (SCADA) system: general term for the software system used to remotely monitor and control network infrastructure (substations, lines, DER...).

Universal Terrestrial Radio Access Network (UTRAN): it is a collective term for the network and equipment that connects mobile handsets to the public telephone network or the Internet.

Virtual Private Network (VPN): it enables users to contact across shared or public networks as if their computers were connected to a private network. A VPN is created through the use of dedicated connections, virtual tunnelling protocols or traffic encryption.