D4.1.4.1: Collection of Smart Grid communication requirements

Editors: Holger Elias (NSN), Kimmo Kauhaniemi (UWASA), Timo Knuutila (NSN), Pertti Raatikainen (VTT), Arto Rantala (NSN), Erkki Viitala (Emptele), Sampo Yliraasakka (NSN), Juha Zidbeck (VTT).

1 Abstract

This paper shall give a 360 degrees view on requirements which arise around the public electricity network (i.e. the electricity grid), while evolving from a rather unidirectional distribution network (from electricity source to sink) towards a bidirectional energy network with new eco-friendly power generation and storage technologies, connected at all voltage levels of the network, as well as intelligent electricity users, who control their electricity utilization in an appropriate (smart) way.

Obviously this requires the utilization of ubiquitous, or also called pervasive communication capabilities to all those network nodes generating or consuming electrical energy.
Since ubiquitous communication capabilities are not available in today's electricity networks, we discuss communication technologies and ways how they can be utilized to fulfill.

This includes an introduction to the electrical energy business in terms of roles and tasks of its participants, how the business will evolve from today's rather static operation towards a dynamic (smart) one by organization.

While communication technology exists and evolves in parallel to the smart grid, we give an overview of fitting technologies, which already are available or already visible and suitable.

2 Revision History

Edition	Date	Status	Editor
0v1	18.5.2010	Initial proposal for Table of Contents	T.Knuutila, P.Raatikainen, J.Zidbeck
0v2	16.6.2010	Initial text to some chapters	E.Viitala , J.Ekholm
0v3	10.8.2010	Added input to Chapter 8 about SoA	P.Raatikainen, J.Zidbeck
0v4	25.8.2010	Reformulation of table of contents	T.Knuutila, E.Viitala, P.Raatikainen
0v5	15.9.2010	Input to sections on Security and Home Networking	H.Jormakka, P.Raatikainen, J.Zidbeck
0v6	16.9.2010	Input to sections "Generation" and "Communication Business Models"	E.Viitala
0v7	23.9.2010	Minor editing including an initial component for section "Communication network components available/applicable to smart grids"	P.Raatikainen, J.Zidbeck
0v91	6.10.2010	NSN deliverables added and updated (Use cases, Life Cycle Requirements)	H.Elias
0v92	10.10.2010	Components for section "Communication network components available/applicable to smart grids"	P.Raatikainen, J.Zidbeck
0v93	11.10.2010	Mod's to chap. 4.1 ff: Communication Business Models	E.Viitala
0v94	12.10.2010	Chap. 5.2 added, changes made during todays review	Team + E.Viitala, T.Knuutila, H.Elias
0v95	13.10.2010	Updated Table 1 under Chapter 5 with LTE/LTE-A and added respective SoA at end of Section 5.1 Minor text editing in chap. 5, format to final layout	P.Raatikainen, J.Zidbeck, H.Elias
0v96	14.10.2010	Chap. 2.9 & 3.5 & IEC61850-3 environmental standard reworked/added (to new chap. 4.14.4) plus formatting	E.Viitala, S.Yliraasakka, H.Elias
0v97	1.11.2010	Summary, spell & language checking	T. Knuutila
0v98	2.11.2010	Modifications & corrections by Kimmo Kauhaniemi included	T. Knuutila
0v99	2.11.2010	Abstract added, PON technology mentioned in chap. 8.2.3, final format editing	H.Elias
0v992	8.11.2010	Added more Abbreviations into Appendix. More editing and formatting	P.Raatikainen, J.Zidbeck H.Elias
0v993	14.11.2010	Adding "conclusions"	T. Knuutila
1v0	30.11.2010	Version change to 1.0, no changes	T.Knuutila

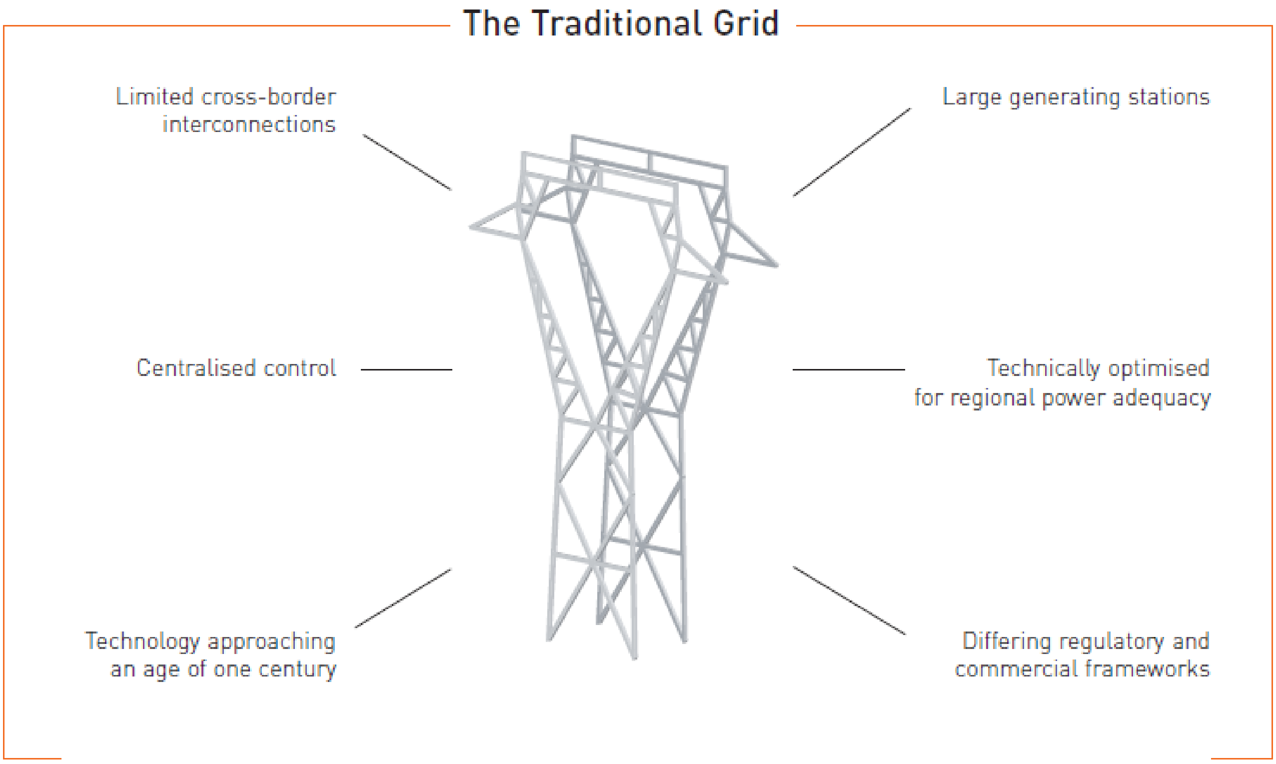
D4.1.4.1: Collection of Smart Grid communication requirements

3 Table of Contents

4 Background

From EU perspective (according to European Technology Platform – Smart Grids initiative) today's grids are predominantly based on large central power stations connected to high voltage transmission systems which, in turn, supply power to medium and low-voltage local distribution systems. The transmission and distribution systems are commonly run by natural monopolies (national or regional bodies) under energy authorities' control. In contrast, the generation sector is increasingly competitive.

The overall picture is still one of power flow in one direction from the power stations, via the transmission and distribution systems, to the final customer. Dispatching of power and network control is typically the responsibility of centralized facilities, controlling several regions from one place. There is little or no consumer participation and no end-to-end communications.



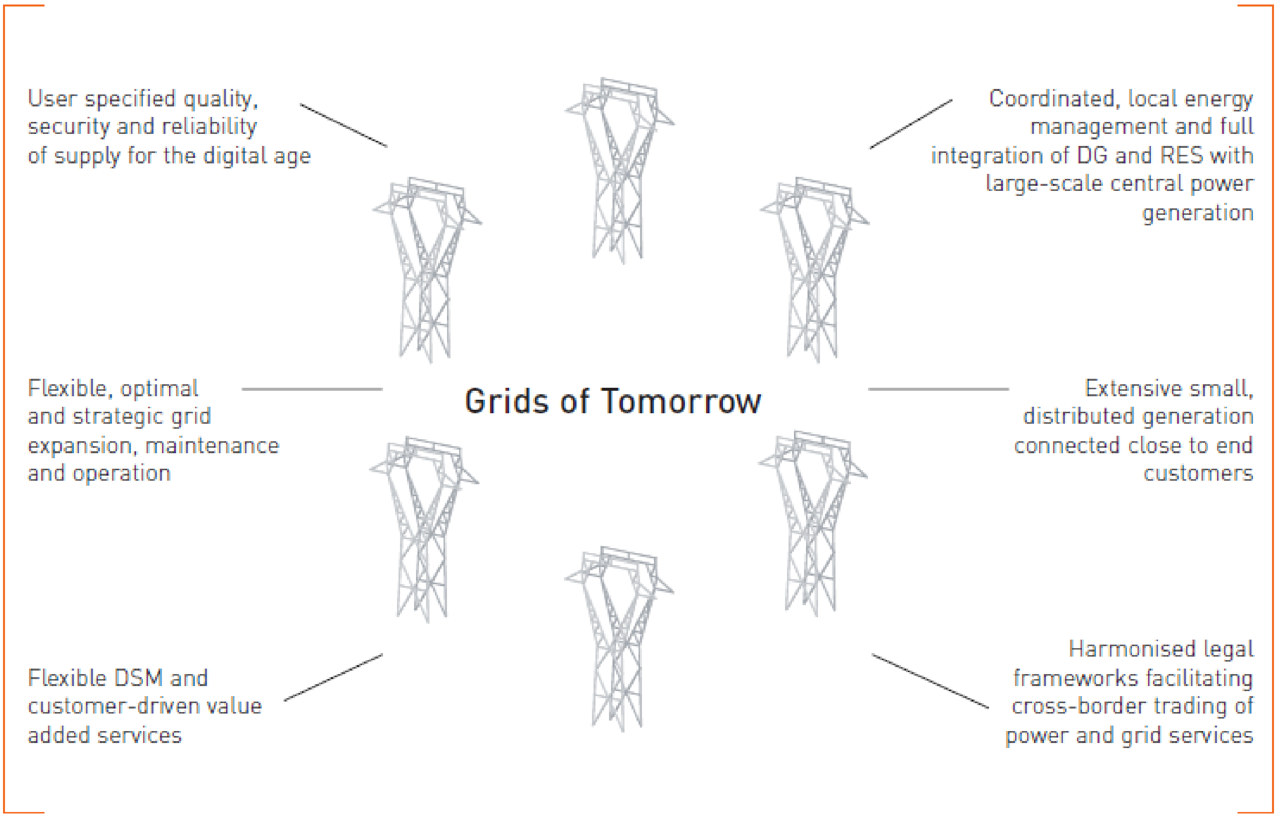
Traditional grid design has evolved through economies of scale in large centralized generation and the geographical distribution of generation resources (locations near coalfields, cooling water, hydro resources, etc). The grids were optimized for regional or national adequacy. Interconnections were originally developed for mutual support between countries and regions in emergency situations, but they are increasingly being used also for trading between states.

The transmission grid provides an arena that has traditionally enhanced the overall reliability of power supply. The existing grid system provides an excellent foundation from which future challenges and opportunities can be met.

However, the change should be accomplished through an incremental rather than a revolutionary approach and so the design of a long-term strategy is indispensable. *Source /1/.*

Future grids

Distribution grids will become active and will have to accommodate bi-directional power flows. The European electricity systems have moved to operate under the framework of a market model in which generators are dispatched according to market forces and the grid control centre undertakes an overall supervisory role (active power balancing and ancillary services such as voltage stability). Distribution networks, on the other hand, have seen little change and tend to be radial with mostly unidirectional power flows and ”passive” operation. Their primary role is energy delivery to end-users.



Future models for the electricity grids have to meet the changes in technology, in the values in society, in the environment and in commerce. Thus security, safety, environment, power quality and cost of supply are all being examined in new ways and energy efficiency in the system is taken ever more seriously for a variety of reasons.

New technologies should also demonstrate reliability, sustainability and cost effectiveness in response to changing requirements in a liberalized market environment across Europe.

In the future operation of system will be shared between central and distributed generators. Control of distributed generators could be aggregated to form microgrids or ‘virtual’ power plants to facilitate their integration both in the physical system and in the market (figure below) *Source /1/*

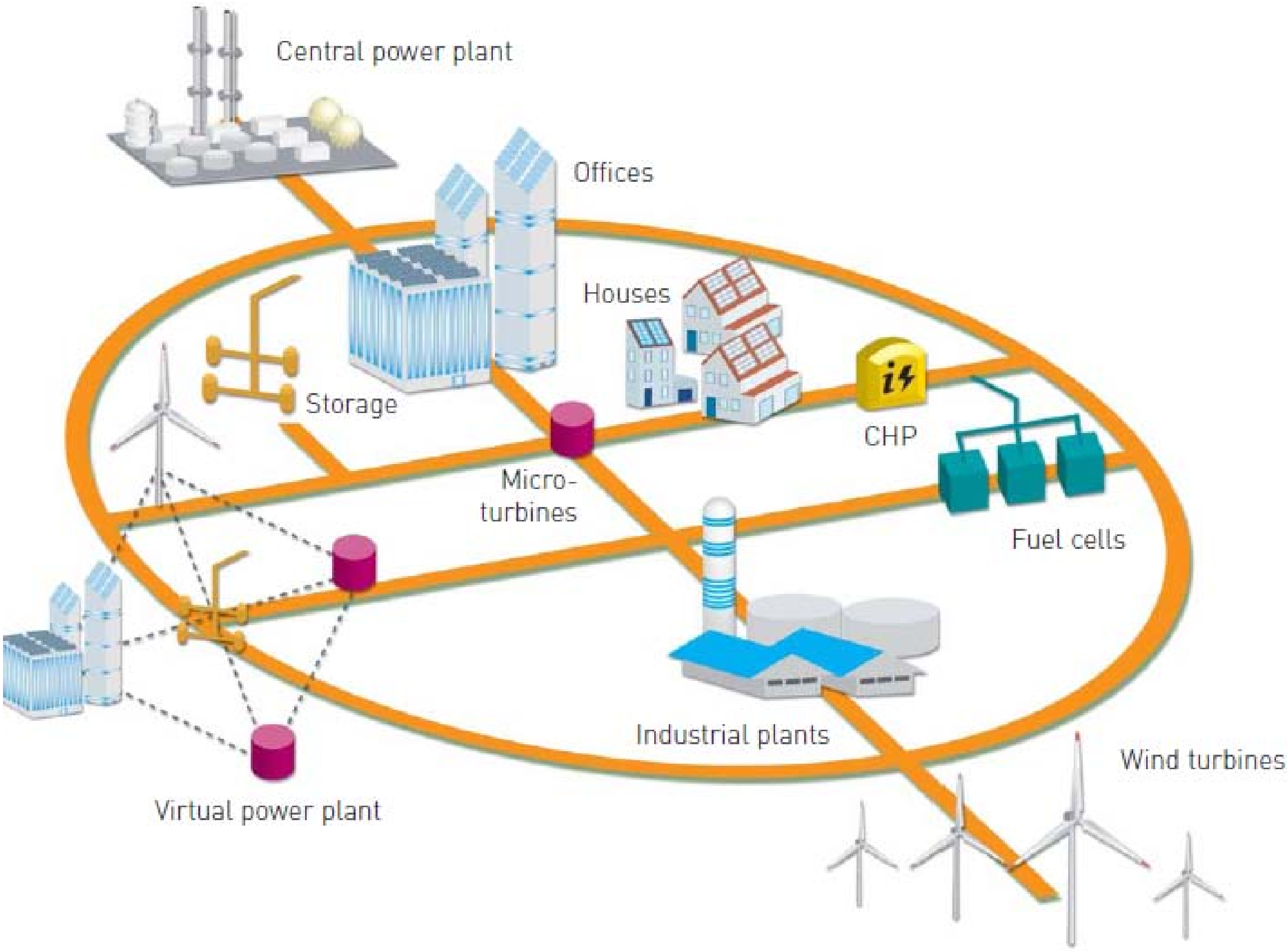


Figure: Future power grid

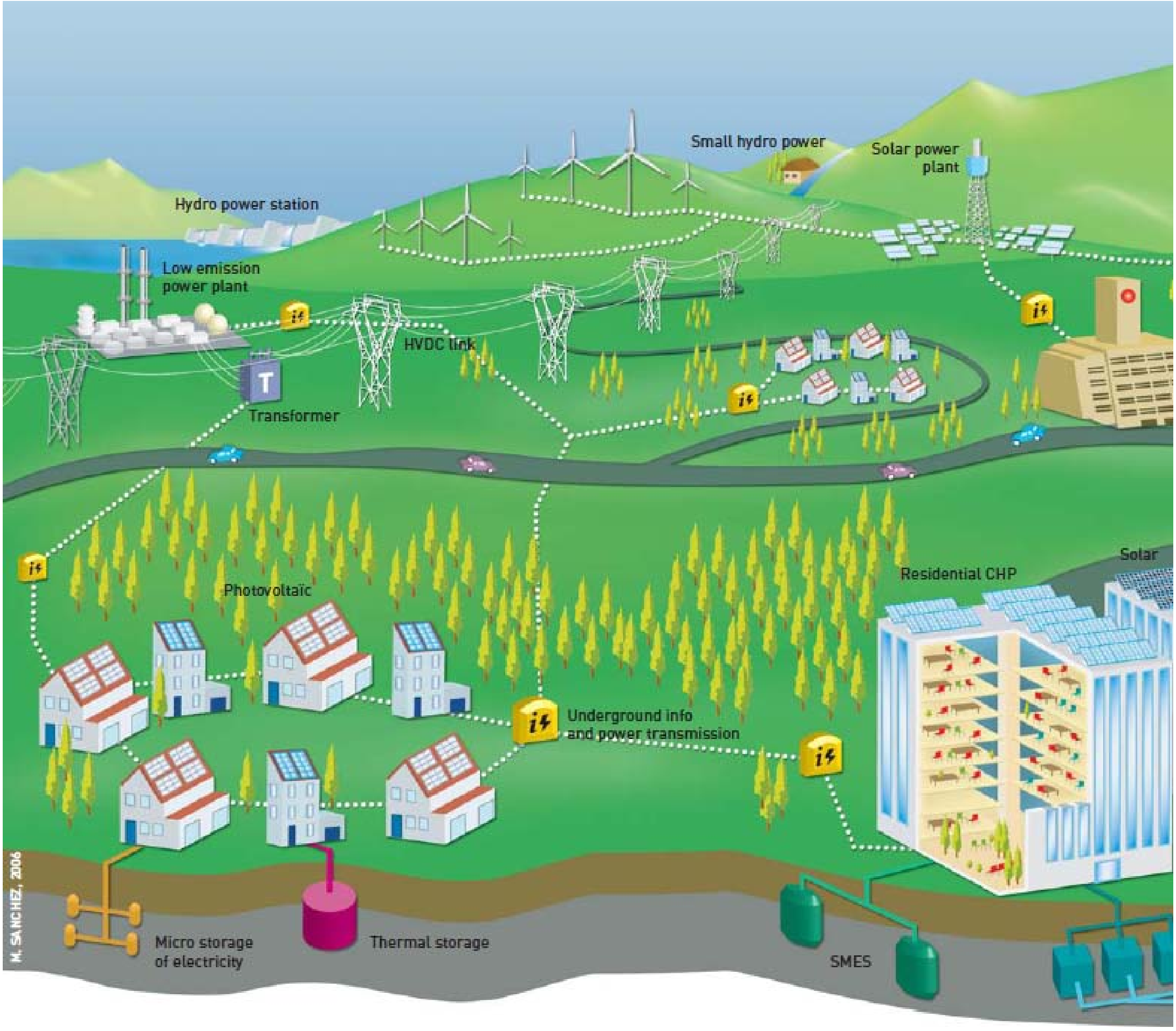


Figure: Vision for future power network – Smart Grid

The goal of this document is to analyze data communication requirements both for the traditional and future power networks – smart grids.

5 Overview of Service/Business Domains

5.1 Current Electricity Market

In addition to Great Britain, Sweden and Norway, Finland has been among the first countries to open its electricity market to competition.

In Finland, the market began to open up in stages in 1995. At that time, electricity production and sales were separated from electricity transmission and distribution, the business operation of which is subject to license. Since 1998, also households have been able to request for tenders from electricity suppliers. Tenders cannot be requested for electricity transmission and distribution. Consumer would not benefit from the construction of several parallel electricity networks.

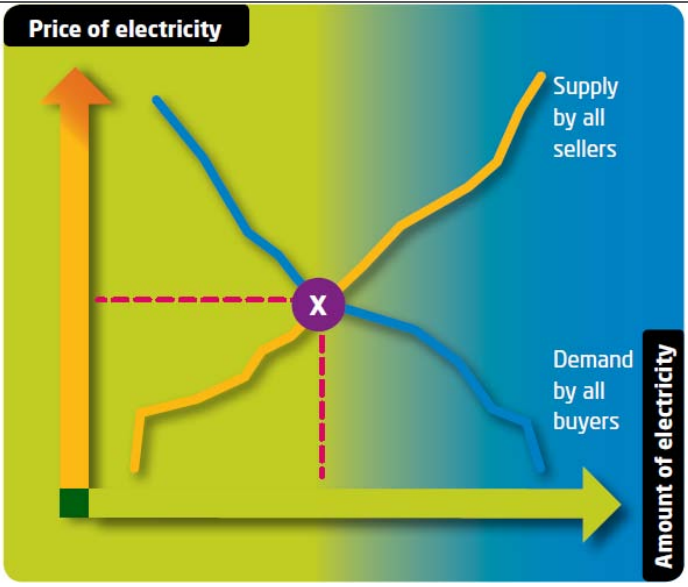
The Nordic electricity market is functioning well. Opening of the market to competition has been facilitated by the fact that there have traditionally been a lot of electricity producers and suppliers in the Nordic countries. Industry is also a significant electricity generator, especially in Finland. Today, there are more than a hundred companies producing electricity, just under a hundred electricity suppliers and hundreds of power plants in Finland. Conversely, the electricity market in many European countries is still fairly concentrated despite the fact that they have opened their electricity market to competition.

	Electricity flows from the power plants to consumers, such as homes and factories, via the electricity network. The network companies take care of electricity transmission. The producers sell electricity to the exchange, to retailers or direct to major customers.

In the wholesale market, electricity is traded on the power exchange. The wholesale price of electricity is determined according to supply and demand. Approximately 70 per cent of the electricity consumed in the Nordic countries is traded on the Nordic power exchange.

The Nordic power exchange was first established in Norway in 1993 when the electricity market opened to competition in that country.

The exchange started to expand by degrees, in Finland in 1998. The Nordic power exchange, Nord Pool Spot, is owned by the Nordic transmission system operators, in Finland by Fingrid Oyj.



Electricity is first transmitted from major power plants to Fingrid's main grid. Fingrid is responsible for ensuring that the electricity system is working throughout Finland and enables the functioning of the electricity market. Fingrid owns Finland's main grid and all significant connections to neighboring countries.

The main grid is a high-voltage network from where electricity is transmitted to distribution networks via regional networks. The distribution networks are divided further into two voltage levels, medium- and low-voltage networks.

Households are connected to low-voltage networks. Local or regional network companies are responsible for the distribution networks. In Finland, there is a total of 380,000 kilometers of electricity network. *Source /2/*

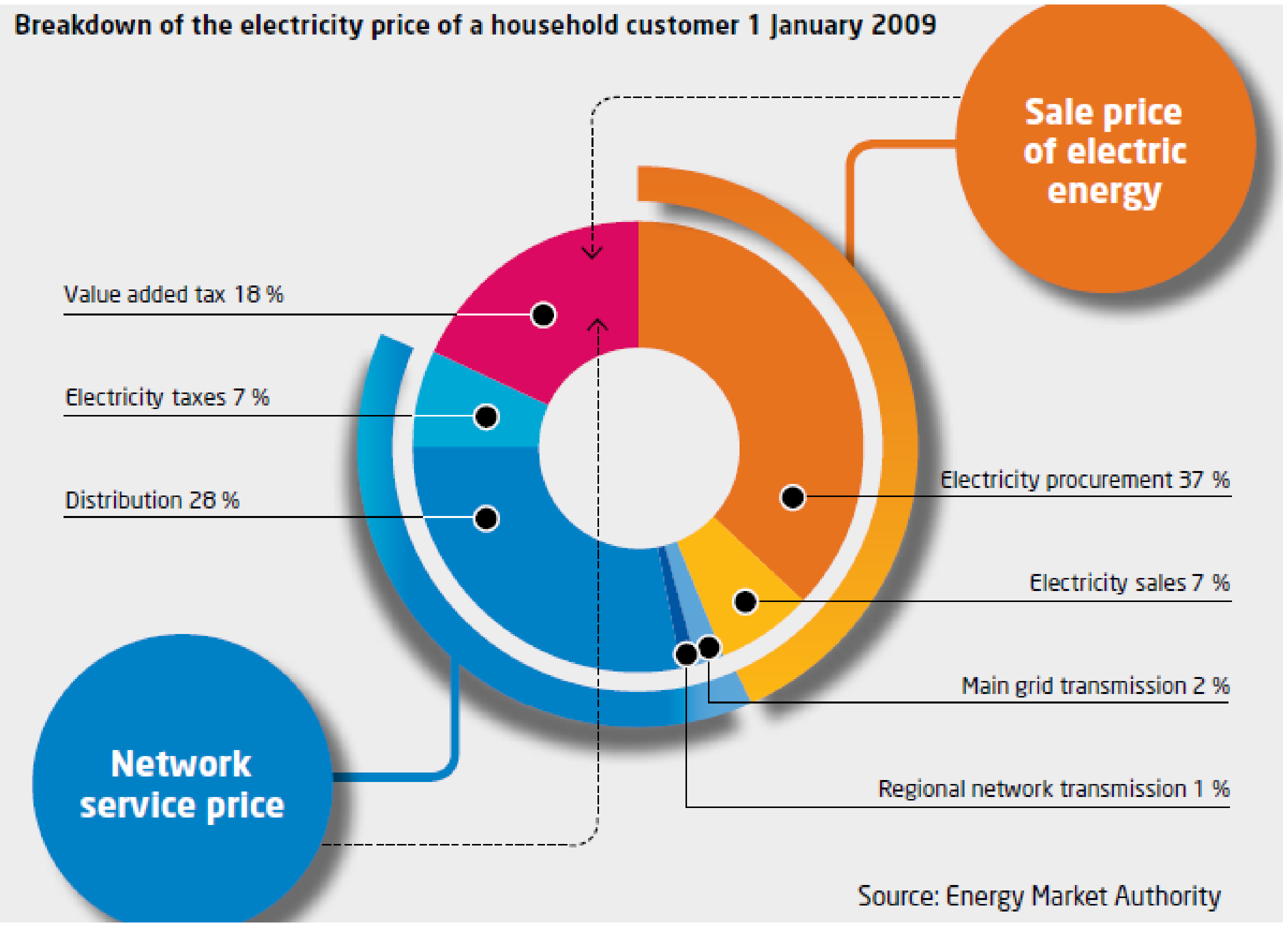


Figure: Breakdown of electricity price

5.2 Generation

Primary energy is unprocessed natural energy. This category includes hydropower, wind, ground heat, solar power, uranium and various fuels like coal, peat, wood, natural gas and oil. Primary energy is divided into renewable (e.g. hydro power) and fossil (e.g. oil) energy.

Secondary energy is refined primary energy such as electricity, district heat, gasoline and fuel oil. Most of secondary energy goes directly to the end use.

More than one third of electricity is produced in Finland by domestic sources and out of that almost half is produced by emission free hydropower. One third is produced by nuclear power. *Source /2/*

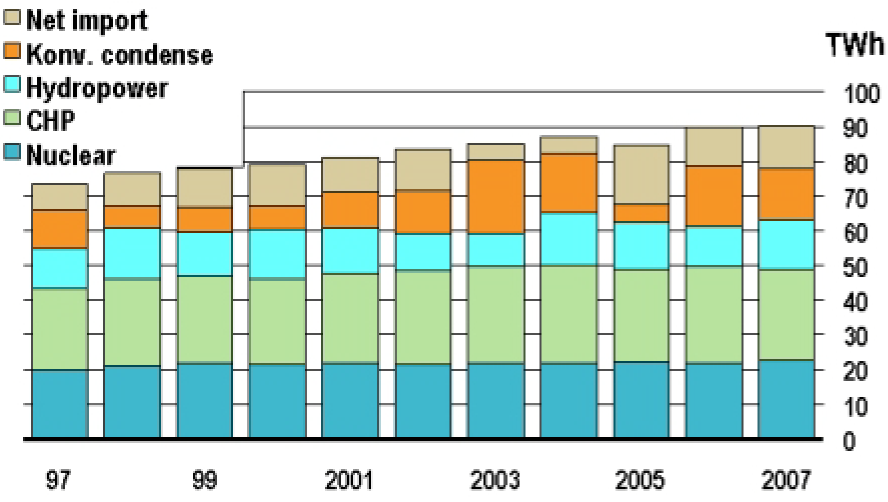


Figure: Electricity sources

5.2.1 Distributed Energy Resources (DER)

Distributed energy resources (**DER**) are small-scale power generation and storage technologies (typically in the range of 3 kW to 10,000 kW) used to provide an alternative to or an enhancement of the traditional electric power system and located near the poin of use.

The cost of electricity (COE) produced by DER depends on the chosen technology. When calculating the COE, various cost components must be taken into account, such as capital, installation and maintenance and fuel costs. In some cases the fuel cost is zero (e.g. photovoltaic) and in some cases the fuel is from local sources with no market value (e.g. waste). Many of the distributed generation technologies are based on primary energy sources that are not available continuously. A good example of this is the wind power. In order to have higher security for the power supplied from such sources it has become evident that some kinds of energy storage facilities are needed. In the following some of the key DER technologies are briefly summarized.

Wind power technology is rapidly developing and the size of the units has been increasing from below 1 kW units up to 5 MW. In the power range below 1 MW a typical de-sign has been the fixed speed stall regulated wind turbine with asynchronous generator. In order to withstand the mechanical stress, most wind turbines above 1 MW are equipped with a variable speed system incorporating power electronics in combination with pitch control.

Photovoltaic (PV) systems are commonly known as solar panels. PV solar panels are made up of discrete silicon based cells that convert sunlight radiation directly to electricity. These cells are connected together in series and parallel in order to give the desired output. A PV panel outputs direct current that is directly proportional to the solar radiation. This current is fed into grid applying first a DC/DC converter in order to achieve desired voltage level and then DC/AC converter to get proper AC output.

Reciprocating engines, developed more than 100 years ago, were the first among DG technologies. They are used on many scales, ranging from small units of 1 kVA to large several tens of MW power plants. Reciprocating engines are usually fuelled by diesel or natural gas. Typically, synchronous generators are applied with internal combustion engines although some examples can be found where induction generators are applied.

The basic combined heat and power (CHP) plant consists of the system with boiler and steam turbine. In the boiler the incoming water is transformed into dry steam under high pressure. The steam is transmitted to the turbine where it expands and as a result the electricity is produced by the generator. The wet steam leaves the turbine and passes through a heat condenser where it exchanges heat with water in the heating system. There are different types of steam boilers and almost any fuel can be used. The average electrical efficiency is about 20 to 30 %, but the total efficiency can reach 80-85 % depending on the efficiency of the boiler, other losses and size of the unit.

Micro-turbine represents a new modular generation technology that is also capable operating in combined heat and power mode. For each produced kilowatt-hour of electricity the micro-turbines will produce two kilowatt-hours of heat. A typical construction of a micro-turbine consists of a turbine mounted on the same shaft as the compressor and a high-speed generator rotor. The shaft spins up to 100 000 rpm. The generated high frequency AC needs to be rectified to DC and then converted back to a three-phase AC with grid frequency.

Fuel cells generate power through the electrochemical reaction between hydrogen and oxygen. The conversion is highly efficient and leaves only water and heat as by-products, which is the main motivation for the increasing interest in the technology. For DG purpose fuel cells from 0.5 kW and upward are developed. All fuel cells generate a direct current and the output voltage depends on the cell voltage and the number of cells in series. Furthermore the voltage varies with the load and also to some extent with time as the fuel cell stack ages. To obtain AC output a DC to AC converter is needed.

5.2.2 Communication in DER systems

A typical feature of DER system is that it is not owned by the distribution system operator (DSO). This leads to a situation where DSO has only little or no information about the local DER systems. Furthermore, in many cases there is only some manufacturer specific communication link between the DSO's control center and the DER unit. Recently the standardization has also evolved in this area and it is expected to bring some new possibilities to realise the Smart Grid concept

As a part of IEC 61850 standards the standard IEC 61850-7-420 has been published 2009, it deals with the complete object models as required for DER systems. It uses communication services mapped to MMS as per IEC 61850-8-1 standard.

OPC is also used for the communication between different entities of DER system

Source /3/

5.3 TSO

In electrical power business, a **transmission system operator** (TSO) is an operator that transmits electrical power from generation plants to regional or local electricity distribution operators.

In Finland the grid operators, monopolies by definition, were given clear rules: the grid operators must make the grid available to any player who wants to use the grid against reasonable compensation. These developments have led to the birth of an authentic electricity market place, which use the grids as a common platform serving all of the competing players on the market.

Fingrid Oyj owns and operates the Finnish high-voltage power transmission network comprising the 400 and 220 kV power lines and the major 110 kV lines and substations.

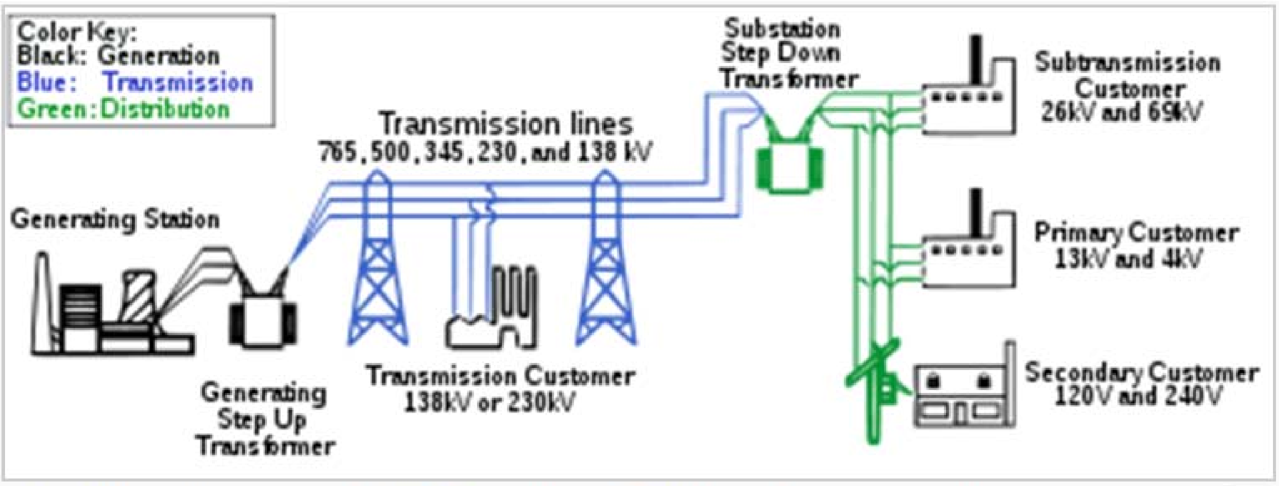
Regional, local and distribution activities are the responsibility of the electric utilities, which are licensed to operate the local grid by the State.

Electricity transmission is priced using a so-called point tariffing system. The user can procure electricity from anywhere in the country without restriction. The user pays one grid transmission fee at his grid point, which covers the transmission costs for the use of the entire grid, without any additional fees. The producer can feed power into the network using the same payment principle. The grid operator is responsible for running, maintaining and developing the network. Source /2/

Transmission system operators use very high voltage (above 100 kV) electrical lines with transformers being used to reduce the voltage to below 66 kV, for electrical power distribution.

Transmission system operators are the backbone of the electrical power grid, and are often wholly or partly owned by state or national governments. Transmission system operators link power generators with distribution companies according to transparent and fair rules. In many cases they are independent of electricity generation companies (upstream) and electricity distribution companies (downstream). They are financed either by the states or countries or by charging a toll proportional to the energy they carry.

Safety and reliability are a critical issue for transmission system operators, since any failure on their grid or their electrical generation sources might propagate to a very large number of customers, causing personal and property damages. Natural hazards and generation/consumption imbalances are a major cause of concern. To minimize the probability of grid instability and failure, regional or national transmission system operators are interconnected to each other. Between them, they are responsible for the overall load management on the main distribution grid.Source /3/



Simplified diagram of AC electricity distribution from generation stations to consumers

5.4 DSO

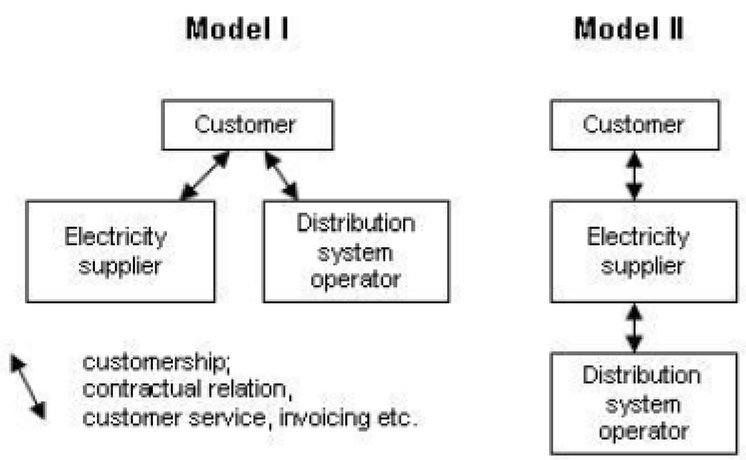


Figure: Simplified retail market models

The DSOs' role is not totally invisible for the customers. They, at the least, conclude connection contracts with the customers. Apart from maintaining and developing the network, the DSOs are in charge of many duties that are necessary for the market to function, for example metering the energy consumption. Invoices based on estimated consumption values still exist in few countries.

In many countries, the DSOs also charge the electricity tax or environmental fees from the customers. The DSOs are responsible for contracting on network connection. Sourve /4/

5.5 Retailer

Electricity retailing is the final process in the delivery of electricity from generation to the consumer. The other main processes are transmission and distribution.

The distribution system operators (DSO) form the link between retailers and customers. The DSOs are responsible for the distribution of electricity in low-voltage networks, for metering the electricity use of end-users and for maintaining the quality of the electricity in the grid. Previously the distributor and retailer have often been the same company. However, in Finland the legislation has now forced the local utilities to form separate companies for retail and system operator businesses.

Although retailing is no longer regulated, some of the retailing companies in Finland are determined obligatory suppliers. This obligation is imposed on a retailer who is in a dominant market position within the area of the DSO. An obligatory supplier must provide electricity to small scale users (main fuse 3x63 amperes and annual consumption of 100 000 kWh at most). This obligation is in place so that all electricity users are guaranteed to have a supplier. Source /5/

5.6 Meter Operator

Metering is in practice done by the DSO. The DSO communicates the values to the retailer which then bills the customer for the correct amount.

DSO may outsource the technical work to a service provider, but owns the meters and customers.

However there are Meter Operators (e.g. in UK) who does the metering.

Meter Operator History

Competition in metering was introduced for larger customers in the electricity market in 1994. Up until that time all metering work had been performed by regional or national monopolies.

As independent Meter Operators entered the market the original metering businesses were separated from their corporate companies. New trading arrangements were introduced to the electricity and gas markets to enable competition in energy supply to develop.

The business interests of Meter Operators were found to be different to those of other parties to the trading arrangements. This resulted in metering companies forming the Association to represent their interests in this evolving market.

Since the creation of the Association in 1996 it has grown to encompass all aspects of electricity and gas metering. In recent years the industry has been considering the benefits of smarter metering for all customers, the Association has been actively involved in debating the necessary changes. Source /7/

Meter Operator provides:

- Meter provisioning
- Meter maintenance
- Meter reading

5.7 Industrial/Commercial Customer

Contracts between industrial/commercial customer and DSO/retailer are made in a similar way as with consumer customers. A customer can select network service provider and energy supplier.

Difference is with the collection interval of meter data.

Customers are obliged to hourly metering when customer has main fuse > 3x63 A (with the exception that the customer is buying from the local supplier and the connection contract has been made before the 1st of January 2005 or the annual consumption does not exceed 5 000 kWh.

5.8 Prosumer

A prosumer is a new role for the customer in energy sector. The word "'prosumer'" has come to mean "consumer/provider," (source /wiki/.).

A prosumer can be industrial, commercial or consumer customer, who has energy source that can be connected to electricity network (sees Ch. Distributed Energy Resources".

A prosumer will take energy from the network and feed energy to network and may have compensation for the energy feeded to network.

In the following is a current role of the consumer customer.

A consumer buys electricity by concluding a contract with the electricity supplier. The contract may be either a single overall delivery contract or separate electricity sale contract and electricity network contract. Usually, customers who have not made their electricity suppliers compete only have one overall delivery contract, and those who have invited tenders have a separate contract for electricity sales and transmission. In Finland, most of the electricity sale contracts for households are valid until further notice. In these contracts, the price of electricity follows the development of the electricity market with a delay. The electricity supplier decides on the timing of price changes and notifies the customer of the change of price at least one month in advance. The period of notice for termination of the contract is two weeks. The consumer can also sign a fixed-term electricity sale contract for one or two years. In this contract, the price of electricity will not change during the contract period. A fixed-term contract also binds the customer, and therefore a new contract must not be concluded during the fixed term. After the fixed term has expired, the contract will continue to be valid until further notice unless otherwise agreed with the supplier. A fixed-term contract may help in balancing the household consumption expenses. The consumer will be able to hedge the electricity price in the same way as an industrial company acquiring derivatives on the power exchange. Source /2/

Consumers are free to buy their electricity from any company which offers to sell into the corresponding area. Of the 74 retail companies, about 40 make offers outside of the area where they are the obligatory supplier. Consumers therefore do have a rather large variety of choice. Changing supplier in practice requires contacting the new supplier and terminating the contract with the previous supplier. If the customer was buying electricity from the obligatory supplier, a contract for the distribution of electricity must be drawn separately when the supplier changes. Often electricity companies offer to take care of terminating the old contract for the new customer Source /4/

5.9 Aggregators

Energy aggregators are licensed by the ISOs & RTOs and individual utility companies to help bring demand response (DR) to the energy marketplace.

Aggregators are gaining steam in the demand response marketplace. They aggregate energy across distributed organizations in order to establish a “virtual grid” where a known amount of energy is available for curtailment. Aggregators reap the associated energy credits available for being on stand-by and reducing customer load when an “event” is called. As the amount of customers increase in this arena, aggregators will need to implement a less manual and more scale-able, automated approach to controlling their customer facilities

Source /6/

6 Usage Scenarios

6.1 Islanding operation

As to the telecommunication requirements the use-case is described here shortly. For more information please see WP 1.4.9 Task Description and deliverables.

Overall purpose is to introduce a generic concept for island operation.

Primary target is to transfer to island operation when there is an interruption in electricity distribution from the main grid. Interruption in electricity distribution is allowed when forming the islanding operation network. Sequence for island creation is following:

1. Local intelligence defining the possible island size and generation capacity needed

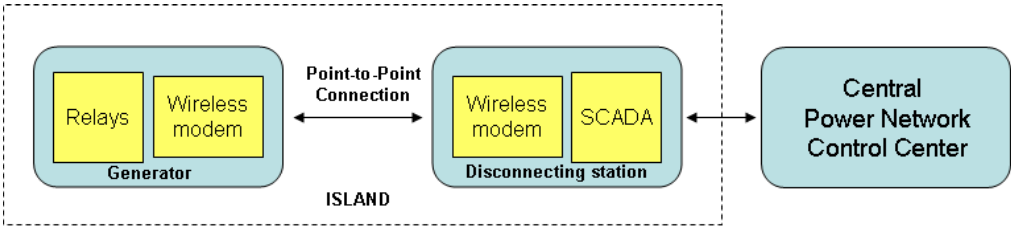
- Adjusting the power of the generation according to the consumption (in case the consumption is low)
- Maximum load estimation – leaving part of the distribution area outside of the island if the power generation not sufficient.

2. Disconnecting the island area from the main network with remote controllable disconnectors.

3. Starting diesel aggregate and feeding the island with it. Island is started with max. 500kW load, because aggregate cannot be started with full load. Therefore only a part of the island is connected to the network first and after a while the rest of it.

4. Connecting the wind turbine also to the island

When the network is in islanding mode, a separate protection scheme must be in use, in order to quarantine safety also in islanding more. If during operation power generation is reduced, load shedding functionality is used for disconnecting part of the island. After the fault situation in the other part of the network is cleared, the islanding area must connected back to the mains network. This reconnection must be done without interruptions in electricity distribution, which means that voltages in islanding area must be synchronized with mains network before the area can be reconnected. After area is connected to mains network, diesel aggregate is shut down, but wind turbine can be left operational and connected. Figure below describes the situation.



Disconnecting station (SCADA) receives status information from a generator. When necessary the station does adjusting or corrective actions. Control center will afterwards re-establish the power network (i.e. connect generator back to network).

Requirements for data communication

Depending on function the following requirements have been identified for the latency.

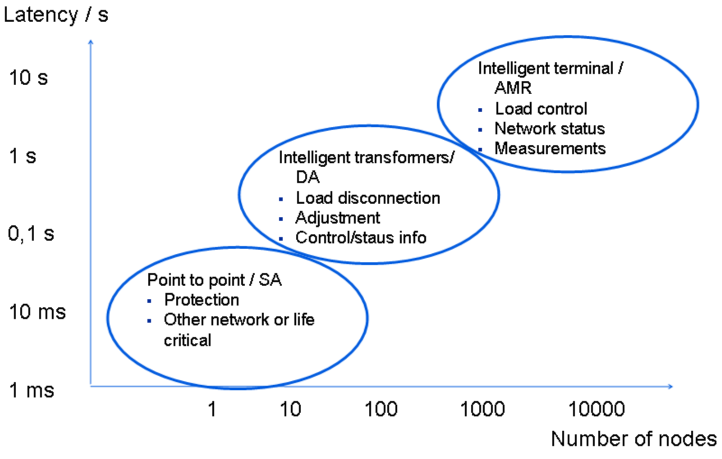


Figure: Latency requirements

In the following table there are theoretical latencies of mobile networks for a subscription.

	2009	2010-2012	2013 ->
GPRS	85kbit/s 200ms	85kbit/s 200ms	85kbit/s 200ms
EDGE	235kbit/s 200ms	235kbit/s 200ms	235kbit/s 200ms
HSDPA	7.2M/2.1M 70-100ms	14.4M/5.6M 70ms	
HSDPA+		42M/11M 45ms	42M/11M 25-45ms
LTE		140M/50M 20ms	140M/50M 20ms

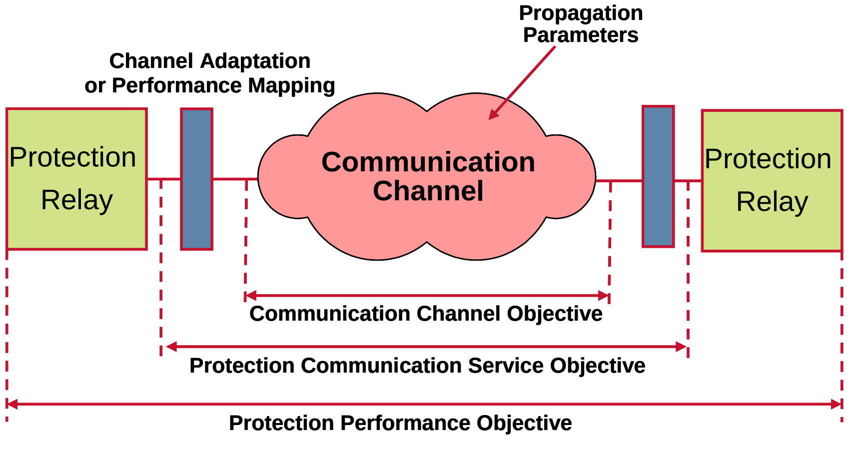
In practise the latency is affected by amount of other users within the same base station, mobile network load and terminals used. Since the point-to-point connection requires two subscriptions, the latency must be multiplied by two. This will indicate that mobile networks could be used for some control and monitoring purposes (table below).

Function	Response time	Data amount	Number of Nodes	What is risked?
Protection	1 - 10 ms	b	1-10	Life
Control	100 ms	B	10-100	Material
Monitoring	1 s	kB	1k	Profit / efficiency
Billing	1 h – 1d	MB	1M	Business
Reporting	1 d – 1 y	GB	1M	Law

For protection fiber or very high speed with very low latency radio links could be used. Some radio links can go as low as 5 – 20 ms latencies (depending on the conditions – forest, hills, weather etc.).

6.2 Protection in Transmission

The following use-case description - Tele-Protection in Transmission Grids - displays the most stringent requirements in the whole grid due to the handling of highest power levels in one area:



At the highest voltage levels, detection of faults and initiation of circuit isolation is required in typically less than one cycle of the power system cycle which means <20ms for a 50Hz system (e.g. Europe) or <17ms for a 60Hz system (e.g. America).

The protection is required 24/7 and so the communications channel must be similarly available; continuously open, connected, and available communications channels are required for electrical power system protection.

Over time, different protection techniques have been developed to take advantage of evolving communication technologies. Some techniques require the communication of “command” information (i.e. ON/OFF signaling); others require the communication of “data” (the transportation of power system signal values across the system), and the necessary characteristics of the communications can differ between these “command” and “data” applications.

Communications channels may be realised in the form of dedicated communications channels (for example, pilot wires, power line carrier, or dedicated fibre-optic links) or they may be leased from telecommunication service providers. Now as we move towards “next generation network” communications technologies, whilst the interfaces presented to the electrical power system protection equipment remain the same, the management of the communications traffic behind the network is dynamic and some of the underlying characteristics reflected in the table that impact the correct operation of the protection, and hence of the operation, of the electrical power system, can no longer be assumed.

An important consideration for each of the different categories of protection scheme is the effect of the communication channel on overall operating times, parameters such as delay, delay variation, errors, channel availability, etc.

Requirements for telecommunication channels are typically specified by local regulator or operator depending on their needs and used protection schemes. Examples of some key requirements for teleprotection in transmission grids are listed below.

Latency e2e 6ms to 15 ms

Latency between traffic directions t_{A-B} and t_{B-A} 0.4 to 0.9 ms

Wander < 0.9 ms

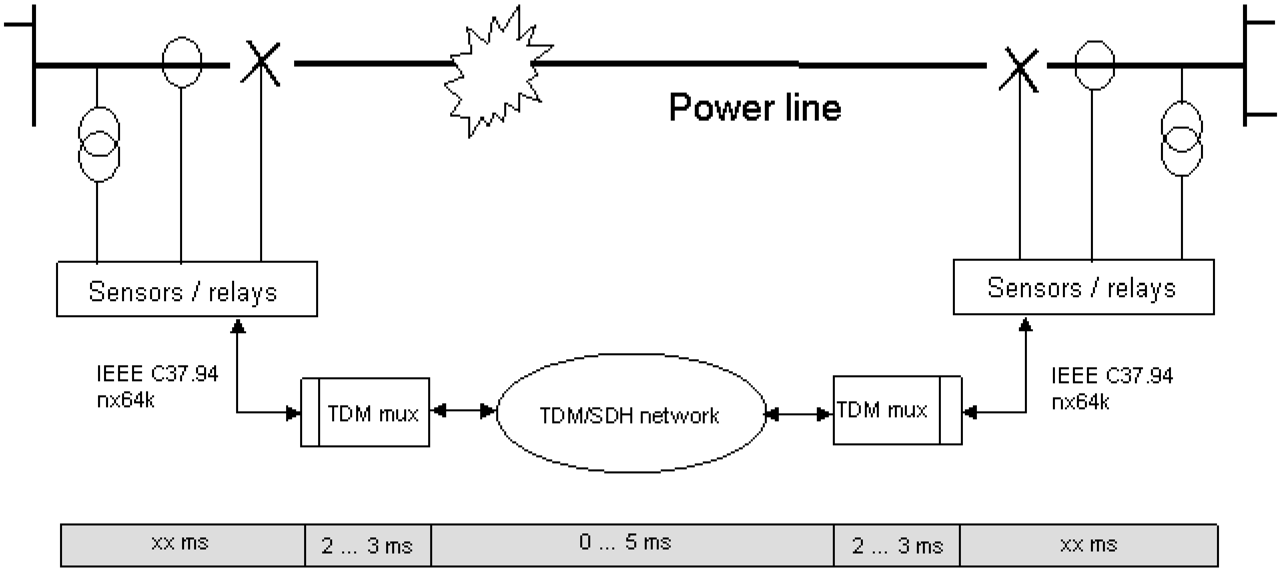
Single failure must not affect to both systems

Protection Switching < 3 ms (not in use by default)

Availability ≥ 99.97% (duplicate system), ≥ 99.9 % (single system)

Mains independent operation 24h

An example of dedicated, command based communication channel using TDM based implementation is shown figure below.



The previous is based on findings described in the document - M2M Mission Critical Thoughts – which determines certain requirements in the field of Smart Grid Transmission related M2M communication. It derives certain time-related values (e.g. latency, throughput, availability, etc.) for the Power Transmission area. Source /9/

6.3 Various Distribution and Prosumer scenarios

The embedded document (see below) determines and describes certain use cases in the field of Smart Grid related M2M communications. Special focus is on Distribution Automation, but it also covers some Prosumer applications. The following selected use-cases are being investigated after a basic introduction:

(Advanced)Distribution Automation area:

WAMS (Wide Area Measurement System)
DER control (Distributed Energy Resources)
DR control (Demand Response)
DS supervision (Distribution System)

Distribution Automation in Transformer Stations (MV to LV) area

DER, DR/Microgrid control

Prosumer (Producer & Consumer) area

Smart Metering
PV generation (Photo-Voltaic)
Home-DR applications (Demand Response) for consumer appliances
PEV charging and power feed

SG-Communications_UseCases.pdf

6.4 Home premises scenario overview

Energy saving, demand response, embedded power generation, interfacing to energy markets, and power quality monitoring at the customer side are all examples of applications and functionalities requiring AMI interfaces to the home. Interval data on consumption may also be needed by various leakage, health, safety, and security monitoring services. In principle, the relevant dynamics of the system in question should determine the time resolutions and time delays. When considering the building energy balances or the load capacity of the electricity grid, the above reasoning typically leads to 3–15 minute time intervals, e.g. at most 5 minute measurement intervals for energy consumption are required for optimizing the energy use in buildings based on the building thermodynamics. Both real time consumption data for immediate feedback as well as historic consumption data supported with expert analysis and performance comparison with peer group need energy saving and reducing CO2 emissions. Real time here means about 1 minute delay and time resolution. Building energy performance benchmarking is the basic and most important comparison service, and it may be implemented as software running in a third party internet portal. This basic budget service can be supplemented by a more expensive expert analysis service. By applying both manual actions based on both immediate and historic information from customer displays as well as home or building energy automation, energy savings are best achieved.

The reduction of energy use and CO2 emissions in the whole energy system is the objective. Focusing to energy end use reduction alone can sometimes lead to wrong actions, because these depend very much on the timing of the consumption in the electricity system. Such wrong action include removing such heat storages which, although locally increase some losses, help to reduce system level emissions by leveling out load peaks. Therefore, especially in the future electricity systems with much intermittent generation from renewables, it is important that demand responds to the situation in the electricity market and grid. Minute level immediate consumption feedback is also best for demand response and interfacing to the energy markets. The electricity market interface needs to be compatible with the time resolution and schedules of the markets participated such as the next day spot market, intra day energy market, and reserves and balancing markets. Although also the costs increase, the value of the demand response is higher on the markets requiring faster response. Also important is to predict the load, its responses and flexibilities accurately for maximizing the benefit and minimizing the risks of market participation, while this typically requires modeling the loads based on minute level interval measurements of the responses.

Many building energy automation and management functions require consumption measurement time resolution better than one hour. These functions include e.g. peak power limitation and thermal dynamics based energy use optimization, which both need 5 minute or better resolution for electricity consumption. Measurement and settlement based on hourly interval data and access over the internet to hourly interval measurements next day for all the electricity market actors is required for at least 80 % of the measurement points of each Distribution System Operator. This includes the consumers and their authorized actors. An essential problem that has been discussed in building automation forums is the need to use own current measurement instruments for immediate consumption feedback.

From the viewpoint of the electricity end user or the whole society in many foreign and international cost benefit analyses and recommendations, compulsory local interface for immediate information has been considered necessary and more than covering its costs. A valid assumption regardless of the system and regulation and legislation, however, the electricity customer is assumed to pay at the end all the costs. No form of smart metering was able to cover the costs of smart metering if the scope of cost-benefit analysis is limited to the distribution network operator only. Lack of adequate open standards for this interface was identified as the main challenge and barrier regarding this interface. Temporary solutions have contributed to the lack of open standard interfaces or any interfaces from the meter to the home network. Also applied by the home automation systems, one of these is optically reading the impulse led of the meter. The fact that the size of the impulse must be changed on both sides simultaneously is a major problem with all impulse reading systems, i.e. the results will be in error when the meter operator updates the meter impulse size. The customers installing their own current measurement instruments in series with the billing meter and typically showing their results as energy is another increasingly popular approach, but suitable only for purposes that tolerate the resulting very high inaccuracy. Consideration may also be needed for responsibilities regarding the safety of the self-made installations. So, it would be better that an open standard Home Automation Network interface is included in the common minimum requirements of a Smart Meter.

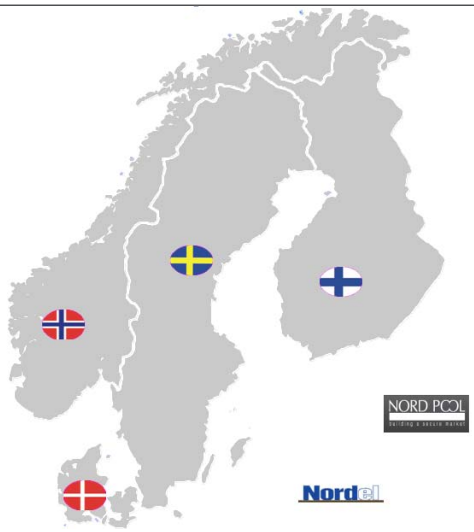
[reference for this above section]
Pekka Koponen, Marja-Leena Pykälä, Janne Peltonen & Pasi Ahonen. Interfaces of consumption metering infrastructures with the energy consumers. Review of standards [Energiankäyttäjien ja kulutusmittausjärjestelmien väliset tiedonsiirtorajapinnat. Katsaus standardeihin]. Espoo 2010. VTT Tiedotteita – Research Notes 2542. 105 p.

6.5 Trading Scenarios

Nordic Ediel Group

In the Nordic Power Market, borders are being eliminated as a result of governmental legislation. Power companies are now operating under new conditions and a larger market for their trade. To operate this market, a huge amount of data has to be interchanged between suppliers, grid companies and system operators. A common standard for Electronic Data Interchange (EDI) is therefore absolutely necessary.

Nordic Ediel GroupWas formed in 2003 to handle Nordic questions related to date exchange in the energy market. The Nordic Ediel Group was founded after Ediel Nordic Forum was reestablished as a pan European body under the name of ebIX, see www.ebix.org.



Nordic Ediel Group has defined few trading scenarios that are between the following actors in the power market describing invoicing and data included in the invoice.

Grid operator: A party that owns one or more net areas and is responsible for the grid services. Also called Net owner.

Supplier of energy: A party that sells energy to consumers.

D4.1.4.1: Collection of Smart Grid communication requirements

Consumer: A party that consumes electrical power bought from a Supplier of energy. The consumer can be a small household or a large multinational company with one or more subsidiaries in one or more countries.

Metering responsible : A party responsible for the metering. This may be the Grid operator or a third party.

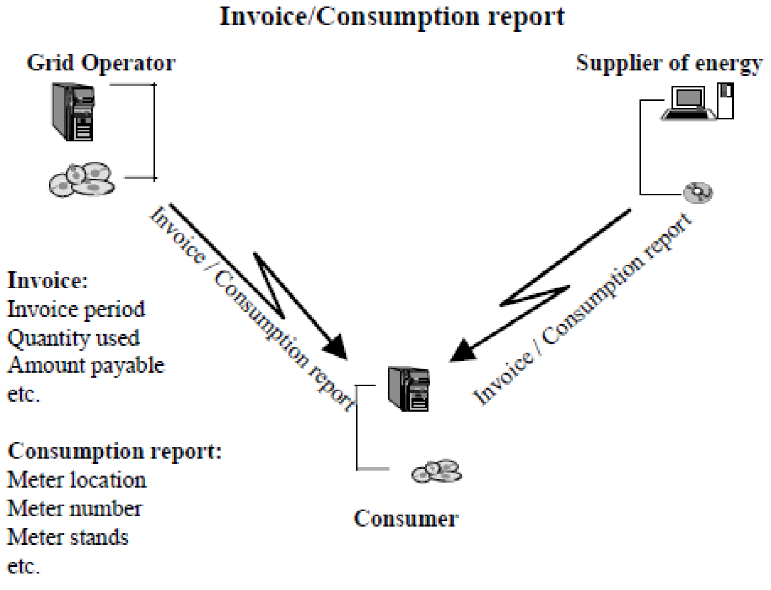
Scenario A

The consumer receives both invoice and consumption report – Each invoice and consumption report concerns one and only one metering point.

The Grid Operator and the Supplier of energy send a consumption report with information about meter stands or time series with metered values in the consumption report, including reporting period, article number, quantity etc.

The Grid Operator and the Supplier of energy send invoices to the consumer. The invoice will contain information about invoice period, invoice quantity, amount payable, product code (GTIN), price etc. The Supplier of energy can also send an invoice on behalf of the Grid Operator.

Normal use of the consumption report will be the matching of the invoice. This scenario will typically be used where the consumer is also using the consumption report for energy calculations and/or statistical purposes.



Scenario B

Scenario B is similar to Scenario A, but gives the possibility to include several metering points in both the invoice and the consumption report. A typical scenario can be where the consumer is a supermarket chain. The supermarket chains head office receives a consolidated invoice (including all metering points from the chain stores). The head office also receives a consumption report containing meter stands or time series with metered values, from all the chain store metering points.

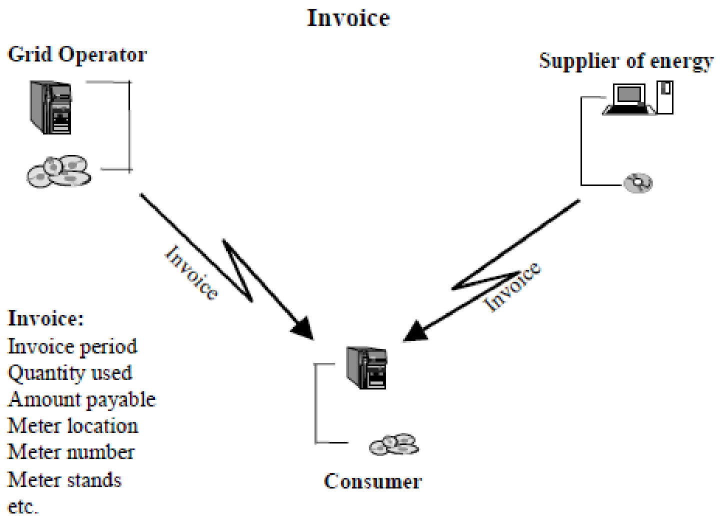
Consumption report:

Delivery point	Delivery point	Delivery point
Metering point	Metering point	Metering point
Meter	Meter	Meter

Scenario C

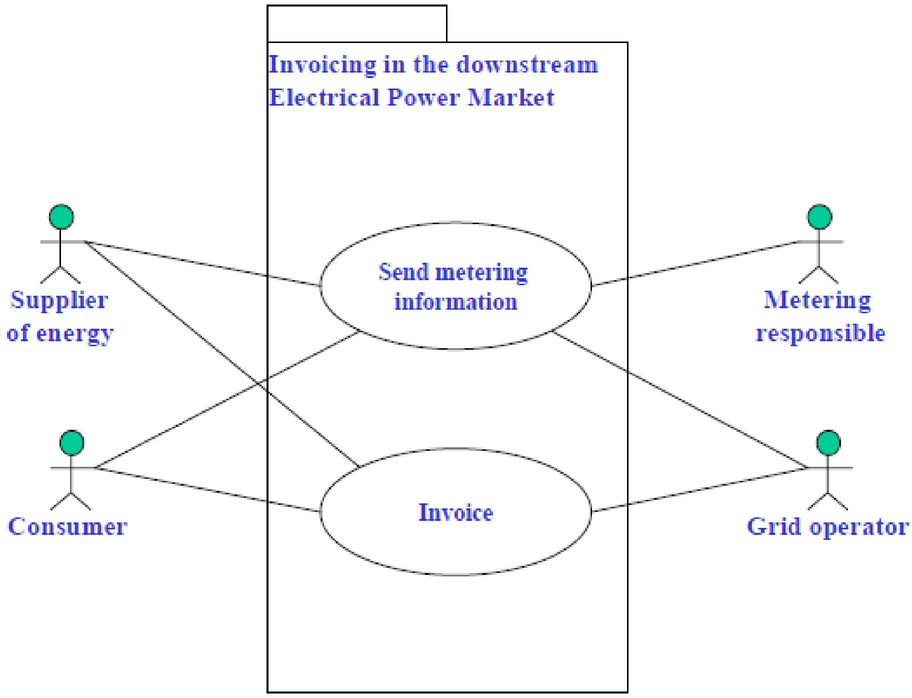
The consumer receives invoices without separate consumption report. The invoice includes meter stands with metered values, for one or more metering points, for one place of consumption.

The Grid Operator and the Supplier of energy sends an invoice message to the consumer. The invoice includes invoice period, metering point identification, invoice quantity, amount payable, meter stands, product code (GTIN), price etc. The consumption report is not used in this scenario.



Use Case Diagram for invoicing

Below is shown a Use Case for invoicing in the downstream electrical power market.



The use case describes the actors participating in the invoicing process in the downstream electrical power market and the interaction between them.

- The following scenario can describe the interaction between the actors:
- The actors exchange partner information, product information and prices.
- The Metering responsible collects metering information from the Consumers.
- The Metering responsible sends metering information (e.g. MSCONS) to the Grid operator.
- The Grid operator sends metering information to the Supplier of energy.
- The Grid operator sends invoice and consumption report (e.g. MSCONS) to the Consumer. This could be done through the Supplier of energy.
- The Supplier of energy sends invoice and consumption report to the Consumer.

If the Consumer complains over the consumption report or invoice the Grid operator and the Supplier of energy must exchange corrections and send a correction invoice or a credit note, new invoice and consumption report to the Consumer.

Alternative scenarios for the upstream market:

- The Metering responsible sends metering information both to the Grid operator and to the Supplier of energy

- The Supplier of energy is sending invoices on behalf of the Grid operator

Alternative scenarios for the downstream market:

The Customer receives both invoice and consumption report (e.g. MSCONS) for each metering point - **Scenario A.**

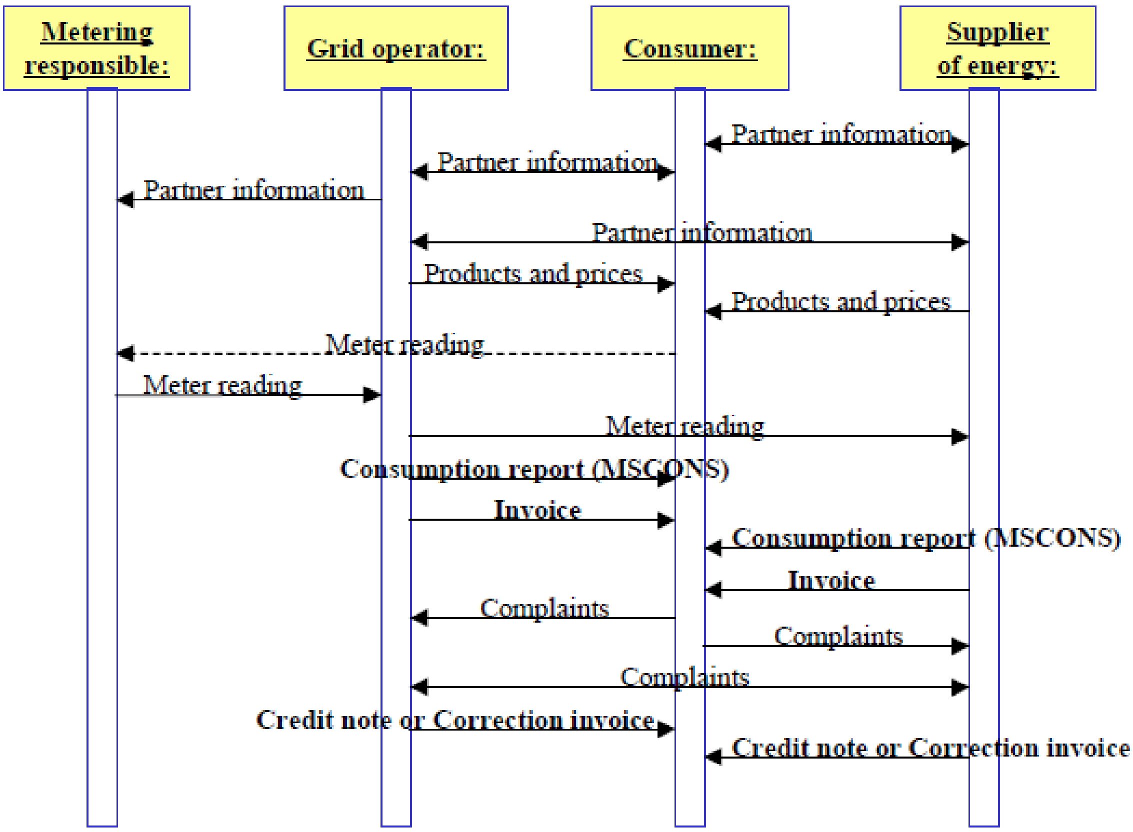
The Customer receives both invoice and consumption report (e.g. MSCONS) for several metering point - **Scenario B.**

The Customer receives only invoice, including meter stands for one place of consumption (premises) with one or more metering points – **Scenario C.**

Sequence diagram for invoicing

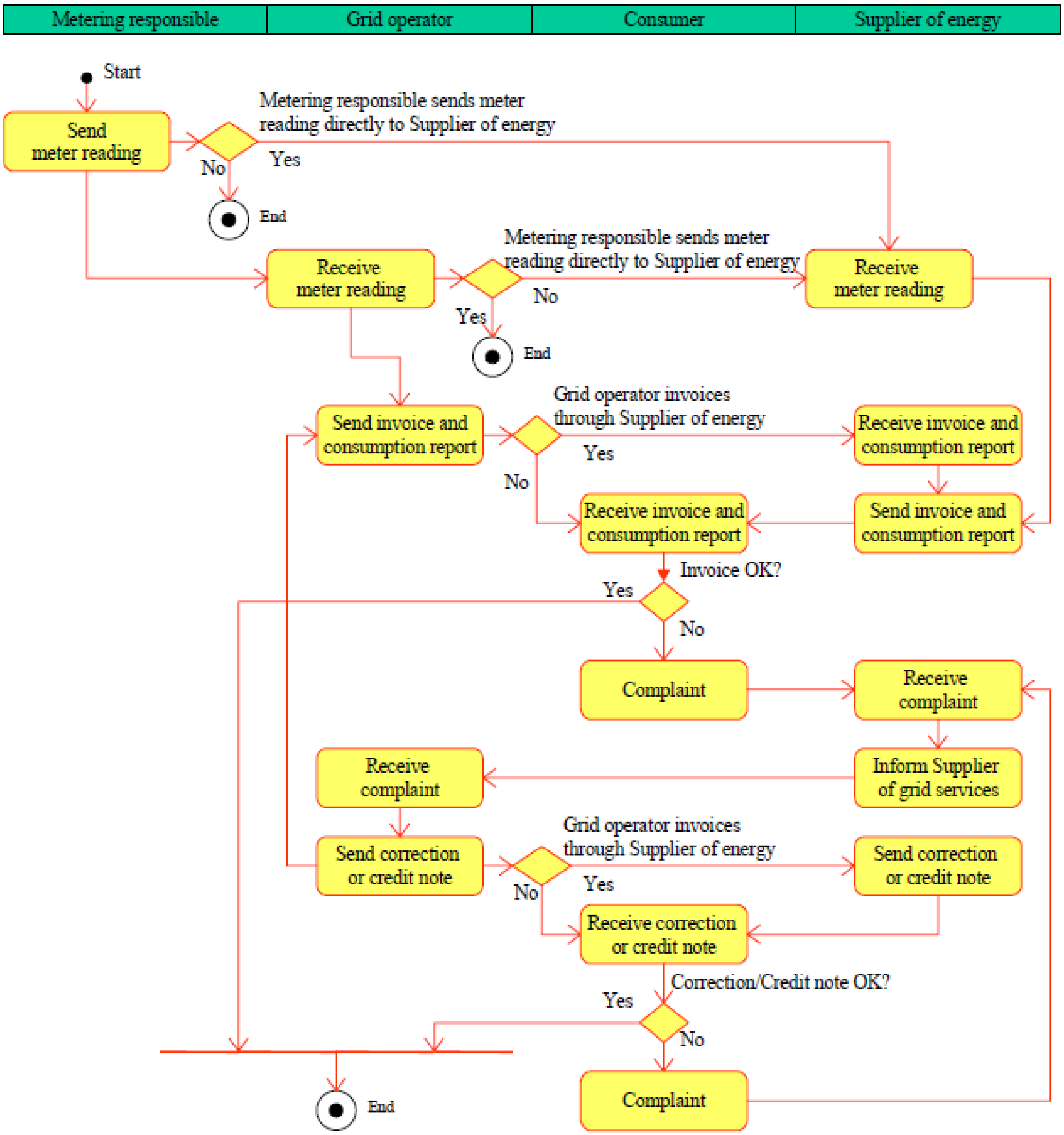
The sequence diagram below shows the information exchanged between the different players in the downstream power market.

The actors identified in the sequence diagram can have different “sub-roles”, such as buyer, seller, invoice issuer, invoicee etc. and a physical company may act as more than one actor.



Activity diagram for invoicing

Below is shown an activity diagram for invoicing in the electricity power market. The activity diagram shows the functional sequence of the invoicing process. Decision points are used to show alternative flows.



Source Business process model for invoicing in the downstream electricity power market (EAN/EDIEL) http://www.ediel.org/ftp/Business%20Process%20Model%20100.pdf

Situation today in Finland

Households may make two types of contracts with retailers: fixed-term or permanent. The maximum duration for a fixed-term contract is two years, and a permanent contract may be terminated by the customer at 14 days notice. The tariff that is applied may be a constant one or time varying. Tariffs may be changed by the retailer at 30 days notice, with notification mailed personally to each customer. Time varying tariffs usually vary within the week (different tariff for day vs. night or weekday vs. weekend) or within the year (winter vs. other season). In principle, consumers are free to choose any supplier they wish and any contract.

Metering is in practice done by the DSO. The DSO communicates the values to the retailer which then bills the customer for the correct amount.

Because customers are metered by the DSO, a retailer wishing to sell electricity outside of its own supply obligation area must communicate with several DSOs in order to obtain metered values for billing purposes.

Customers are billed separately for electricity and transmission, unless electricity is bought from the same company that acts as the local DSO. Billing frequency varies by contract type; some spot-contracts offer monthly billing based on actual use whereas most contracts are still based on billing for example four times a year based on expected use of electricity. The last bill of the year is a settling bill, where the actual use is recorded and accounts settled accordingly.

Consumers are free to buy their electricity from any company which offers to sell into the corresponding area. Of the 74 retail companies, about 40 make offers outside of the area where they are the obligatory supplier.

7 Smart Grid System Requirements

7.1 Communication Business Models

In this chapter few business or earnings models related to utilization of telecommunications services by energy companies are presented.

Telecommunications services are mainly composed of

Devices (modems, routers, terminals) in power network connected to applications (e.g. distribution network control, AMR etc.)

Communication subscriptions and connections (mobile, wireless, fixed) with an agreed amount of service volumes (data, voice, sms, capacity) between devices and applications

For telecommunications services typical added value services can be offered, e.g.

Network control

QoS reporting

Support and maintenance through a service desk

VPN and security

Network planning, delivery/installation.

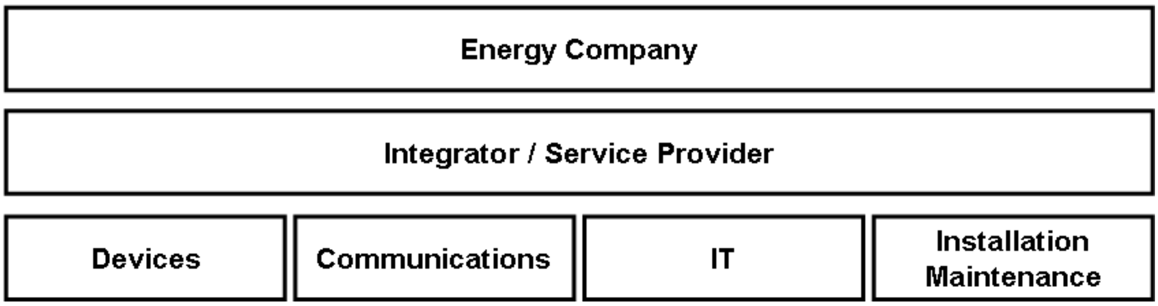
More advanced added value service can be information collection and processing such as AMR including all the above mentioned services with telecommunication infrastructure for tens to hundreds of thousands meters.

The service provider can productize and packet the services to easily sellable, installable and manageable entities, e.g. 3G + modem with flat fee for 12 months, or up to 10 of 1-2 Mbits subscriptions including VPN, email and server disk space 10 Gb plus supervision and so on.

7.2 Players

For the entire telecommunication service, where tens to hundreds of thousands subscriptions with relevant other services will be implemented, many players/stakeholders are needed, e.g. :

- Integrator who builds the solution (can be energy company or outsourced)
- Consultants for specific issues (radio network planning, address management, etc.)
- Telecom operators (mobile, satellite, fixed, fixed wireless) for connections and subscriptions
- Modem and router vendors
- Miscellaneous material vendor (batteries, wires, pylon/tubes etc)
- Logistic companies for transporting
- Recycling companies
- Project houses (installation and field maintenance and support)
- Service Center / Service Desk
- Hosting houses for running servers (network control, field force management etc.)
- SW and HW vendors (network control, field force, trouble ticketing etc.)



7.3 Business / Earnings Logic Examples

Possible business logic or earnings model varies case-by-case depending on customer's own capabilities to take response for parts of the service.

There are three possible models:

full outsourcing

partial outsourcing (e.g. field installation, support and maintenance outsourced)

DIY model, where customer selects vendors and manages all from delivery to support and maintenance.

It is assumed that full outsourcing will be the model of the future, due to the knowledge and expertise needed and due to increasing complexity of technology and less own people at field.. Full outsourced model is where the service provider takes full responsibility for the whole entity, e.g.

The whole data communication network including telecommunication services, their planning, delivery, support, maintenance, spare parts with a certain SLA.

AMR solution so that service provider produces only meter data and takes care for the whole AMR infrastructure with agreed SLA

The service provider manages all other stakeholders (telecommunication network operators/virtual network operators, device vendors, logistics, recycling, project houses, server hosting houses and so on). The service provider pays for the service the subcontractors provide for the total service and receives compensation, if SLA is not met.

The money flow (what is paid, how much and how often) between stakeholders can be based on different types of earnings logics. Ultimate models are (figure below):

Regular payments from customer to service provider. Usually model includes SLA and sanctions, if SLA not met and/or bonuses if SLA exceeded.

Customer pays only, if the service gives a before hand agreed costs savings or wins. The service provider will get an agreed percentage from saving and/or wins. In this model service provider takes the risks and must propagate risks to its subcontractors, i.e. "no money to me, no money to you".

The first model is used with different variations, e.g. customer pays more in advance or pays a certain amount to cover service provider's investments first.

In the latter model service provider must have a thorough knowledge about all possible risks and issues and agree clearly on triggers for payment. Perhaps the model will not be used for communications services but it could be possible in the distributed energy production. The model was introduced to raise questions and possible ideas among readers. It is proposed that deeper analysis about the usability of this model will be left for the next SGEM phases.

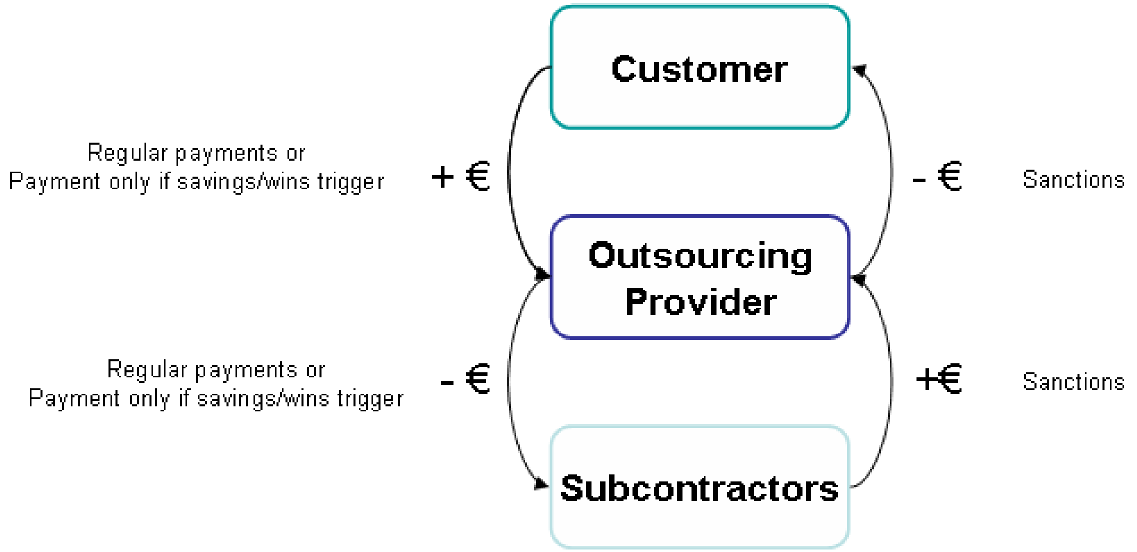


Figure: Money flow between stakeholders

7.4 Life Cycle Requirements

7.4.1 History

Several events around the traditional way of generating and distributing electrical energy, originating by the change of the millennium, led to the EU´s 20-20-20 targets from 2007.
They ask implicitly for the reduction of fossil based power generation and explicitly for the implementation of renewable power generation.
Comparable programs became popular in the U.S. and Asia, also based around the foreseen global environmental impact of excessive CO2 emission, amplified by the uprising demand for energy in developing countries

20-20-20 Targets, as endorsed by the EU Heads of State and Government in 2007 to become reality in 2020:
- A reduction in EU greenhouse gas emissions of at least 20% below 1990 levels
- 20% of EU energy consumption to come from renewable resources
- A 20% reduction in primary energy use compared with projected levels, to be achieved by improving energy efficiency.

These targets impact did impact the traditional transmission and distribution system/grid already heavily.

Some 40 years ago, when most of today's existing grid structures were planned and laid out:

"Distribution networks were designed for radial operation and the presence of generation units at distribution level was not considered in the design at all or only for a negligible fraction ("fit and

forget" approach). Integrating large amounts of distributed generation in actual networks does lead to serious concerns about reliability, quality of supply and voltage control"
(From the Council of European Energy Regulators, Ref: C09-EWG-51-01).

Therefore history originates from centralized systems of generation and distribution architectures towards more decentralized and networked future ones.

7.4.2 Operation Time

The traditional approach ("fit and forget") of the "static & unidirectional" distribution networks infrastructure must be regarded as partially obsolete in the context of the Smart Grid.
Since Smart Grids are still in the evolutionary phase and will maintain their dynamic nature in the far future due to locally changing generation and demand profiles, key investment elements need to be protected in their business case for reasonable amortization periods of 10-20 years. Key elements meant are local transformers, but also line sections, which are difficult to acquire. Due to legal obligations concerning the generation of renewable energy of typically 20 years, distribution network investment schemes need to follow.

Despite the fact that monitoring and control electronics will have a much shorter life-cycle of typically 3-5 years, electronic component standardization and modularity must be maintained accordingly.

Anticipating the below mentioned Gas-Turbine or Storage facilities, their amortization needs to be aligned with the above as well.

Summarizing the above findings, depreciation requirements will probably impact the design of key elements in the Distribution Grid towards lower initial cost at the expense of expected lifetime, i.e. stepping down from > 50 years to >20 years Meantime to Failure (MTTF; e.g. for Transformers).

To cope with this dynamic future, modularity must not only be the key element for local investment (plants, stations), but also for geographical layout of line sections, including communication capabilities alongside.

7.4.3 Upgrading, Evolution

Basically the above mentioned causes a large impact at least on the Medium and Low Voltage distribution grid, which needs to be operated in a reliable bidirectional way, right from the Low Voltage level, as already encountered in areas with high Photo-Voltaic penetration (like in southern Germany).

Further implications, also caused by larger renewable power generation (like Off-Shore Wind-Turbine parks), lead to design changes of the Medium Voltage Distribution Network layout.
A new Distribution Network layout has to encompass temporarily required back-up power sources, like Gas-Turbines or Storage Facilities as well, to cope with the statistical variation of natural energy sources.

Last but not least the High Voltage Transmission network has to take over new functionality in terms of back-up and exchange tasks between political, commercial or adjacent geographical areas.

All of the above changes in operation go hand in hand with the knowledge about the grid's operational status. The better the network is monitored, the better it can be controlled to insure the required reliability, quality of supply and voltage control.
From the level of Syncro-Phasors (PMUs) measurement in High and Medium Voltage Networks down to accumulated data from Smart Meters in local Low Voltage Networks, every node point should become visible and controllable by Networked Management Solutions.
This may be initially achieved best by the extensive utilization of wireless mobile broadband communication solutions, which do not rely on specific layout. The above will also shape additional and most probably different Life-Cycle Requirements to the elements building the grid and to their operation as compared of today.
In such a highly networked environment like the Smart Grid, bringing many different business partners together, seamless interworking is a key factor.
This asks ultimately for the division of the key responsibilities and outsourcing towards commonly trusted parties, which fulfill the business need of all engaged partners equally. Examples are the already mentioned Smart Grid Communication aspect, but could extent also towards maintenance aspects of parts or elements in the Smart Grid. E.g., why should a Smart Grid Operator care about maintenance cycles for the involved infrastructure, it is not a key task to him and also it may span across several business partners' equipment in the grid. Therefore a work-sharing type of eco-system will evolve around the Smart Grid, which will cover individual life-cycle requirements of the grid's logical architecture to be managed independently.

7.5 Security Requirements

The control systems of the traditional grids have been for many years isolated not only from the public networks, but also from administrative corporate networks due to heterogeneous proprietary networks and security concerns. Recently the situation has changed. Due to the increasing complexity and integration as well as the necessity to improve effectiveness of business and production in a highly competitive environment where fast communication and data exchange are crucial factors, the use of communication networks, open technologies and protocols in control systems for critical infrastructures is increasing. The situation will be even more complex in Smart Grids where the ICT network and services provide a real time control and management of energy production and consumption. Customers will work closely with the utility to manage energy usage, sharing more information about their usage of energy what will expose them to privacy attacks. Some of the Smart Grid customers may use public networks, but the Smart Grid as well will be connecting private networks, including home area networks with varying level of security, where firewalls are constrained in their compute capabilities to keep costs down, which may limit the types and layers of security which could be applied with those devices. Many of the networks' gateways will be accessible by many different vendors and organizations with unknown corporate security requirements and equally variable degrees and types of security solutions. Even if one particular interaction is "secure", in aggregate the multiplicity of interactions may not be secure.

E.g., one of the areas of vulnerability for large scale Internet environments lies in the area of inter-domain routing. Routing protocols, and in particular, inter-domain routing protocols can be subject to attacks and threats that can harm individual users or the network operations as a whole.

The communication networks will be opened to external threats typical for any information technology system. Increased complexity of the system is caused by the fact that the operation of the power system must continue 24x7 with availability approaching 100% regardless of any compromise in security or the implementation of security measures which hinder normal or emergency power system operations. Smart Grid operations must be able to continue during any security attack or compromise, must recover quickly after such an attack or compromised information system. Additionally, testing of security measures cannot impact power system operations. While security solutions have been designed for security issues of traditional IT systems, they have to be carefully adapted to demands of Smart Grid environment. Until recently, communications and IT equipment were typically seen as supporting power system reliability. However, increasingly they are becoming more critical to the reliability of the power system. It has to be remembered that in traditional grids the IT system's main task was to provide reliability of the power grid with power availability as a major requirement, why information integrity was a secondary although increasingly critical requirement. With smart meters, confidentiality and integrity of customer information is also important, as it used in the billing processes. Although the traditional grid security technology is focused mostly on accidental/inadvertent security problems, such as equipment failures, employee errors, and natural disasters, existing technologies can be used and expanded to provide additional security features.

Few following sections present Smart Grids requirements grouped according to security threats categories and can be used as guidelines for implementation of a secure system.

7.6 Access control related requirements

One of the main cyber security threats is unauthorized access to Smart Grids elements and services due to disclosed or stolen, e.g. by phishing, users passwords. Not long ago in the traditional grids control rooms it was common to use one password per device what disabled user authentication. Although the situation has changed, there is still objection against regularly changed passwords and the passwords are often easy to guess. [oman] presents interesting data concerning comparison of time used for cracking password using brute-force and dictionary attacks in case of 4, 6 and 8 characters. The measurements were made for a typical substation Controller, but the ratio of the time required in the above cases remains the same in case of any networked device.

To prevent unauthorized access to a system, the system should fulfill the following requirements:

- User identification, authentication and authorization
- Regularly changed passwords
- Avoiding passwords with straightforward dictionary words
- Unsuccessful login notification
- Session lock after number of unsuccessful login
- Remote access policy defined and followed

- Wireless access restrictions
- Access control for portable and mobile devices
- Device authentication and identification
- Access rights specified and enforced – access to unnecessary resources blocked
- Addressing the insider threats, e.g. keeping login records
- Remote session termination possibility
- System presents to a user his account usage and last login

7.7 Data storage and communication security requirements

As Smart Grid means continued expansion of networks to include an even larger number of remote electronic entities, there is required great reliance on shared telecommunications technologies (wireless and standard Internet protocols) to quickly receive and transmit in a secure way necessary data from remote units. Each new source and transmission link not only creates another new entry point for cyber attacks, but also loads operators with managing increases in system complexity. The challenges of keeping up with emerging risks in today's dynamic threat and operating environments require strong protection measures to be successful. These concerns data transferred through communication links, but also protection of sensitive data stored at the grid devices, e.g. smart meters are very attractive targets of malicious hackers, as they are providing data for charging. Compromising meters hackers can change their meters reading data in this way manipulating their energy costs. Additionally, any organization collecting or processing energy usage data and other personal information should ensure that all the data is appropriately protected from loss, theft, unauthorized access, disclosure, copying, use or modification. In addition, given the growing granularity of information from Smart Grid operations, the cyber security must address not only deliberate attacks, such as from disloyal employees, industrial espionage, and terrorists, but also unintentional compromises of the information infrastructure due to user errors or equipment failures. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. To prevent that, data confidentiality, integrity and privacy must be assured and requirements enabling it are:

- Data integrity
- Communication confidentiality
- Cryptographic key generation and management
- Public Key Infrastructure Certificates usage
- Encryption of critical security parameters like sensitive configuration information, passwords, and cryptographic keys
- Denial of service protection
- Protection against replay attacks
- Separation of management functionality from other services
- Security functionality separation
- Data storage protection including sensitive information in portable laptops.

- Protection against malicious code
- Protection against spam
- Error handling
- Use of firewalls, creation of demilitarized zones
- Intrusion detection capabilities
- Portable and mobile devices scanned for malware
- Trusted communication path specified
- Fault tolerant Domain Name Server
- Changes to the system and logs time stamped

7.8 System and access monitoring

Reliable operation of the Smart Grid depends on timely and accurate detection of anomalous events. Power grid operations need sophisticated detection techniques that enable the collection of high integrity data in the presence of errors in data collection. Various sensors in the power/electrical domain already collect a wide array of data from the grid. In the Smart Grid, there will also be a number of sensors in the cyber domain that will provide data about the computing as well as electrical elements. Some of the sensor data should have the possibility to report effects of malicious cyber activity and “misinformation” fed by an adversary, as e.g. smart meters unauthorized disconnection, or meters running backwards. The main requirements concerning monitoring are:

- System monitoring tools used – networks elements regularly or continuously monitored for malicious activities
- Security alerts
- Predictable failures prevention
- Log files of the devices monitored
- Isolation of devices/components that have been compromised, e.g. smart meters with connect/disconnect features allow to disconnect homes from the grid, in case of a security issues
- Anomaly detection
- Systematic backup of critical data
- Logs and their processing tools protected against unauthorized access (possibly in another computer)

7.9 Requirements concerning testing, risk assessment and emergency cases

Absolute security of complex systems is never perfectly achievable, so the costs and impacts on functionality of implementing security measures must be weighed against the possible impacts from security breaches. Balance is also needed between risk and the cost of implementing the security features. Therefore risk assessment has to be based on business rationale and it hast to take into account not only security technologies, but also security policies and security training of personnel. It has to include normal operations and emergency operations when faced with a possible or actual security attack, recovery procedures after an attack and documentation of all anomalies for later analysis and re-risk assessment.

- Assigning criticality and impact levels to smart grid functions/applications to define priorities in case of emergency
- Overriding user rights in case of emergency
- Disconnection in case of threat detection
- Smart meters with connect/disconnect features which allow to disconnect homes from the grid, in case of a security issues.
- Operation critical components identified, replacement in case of emergency provided
- Fast recovery methods
- User-installed software blocked
- New software tested before installation
- Mirror system for critical elements
- Risk assessment policy and procedures
- Vulnerability assessment and awareness
- Testing cannot impact power system operation
- Single points of failure avoided, if not possible identified and risk assessment done

7.10 Defense in depth

It is typically not possible to achieve the security objectives through the use of a single countermeasure or technique. A single security product, technology or solution cannot adequately protect a complicated distributed heterogeneous system by itself. A superior approach is to use a multiple layer strategy involving two (or more) different overlapping security mechanisms, the concept called defense in depth. Defense in depth implies layers of security and detection, even on single systems, and includes the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities along with effective security policies, training programs and incident response mechanisms.

One of the most important security solutions is to utilize and augment existing power system technologies, e.g. SCADA system. Therefore to address new risks associated with the Smart Grid, novel control system architecture designs should provide compulsory segmentation between internal company networks, control systems, and external connections e.g., the Internet, a separation lacking in traditional systems. Innovative architectures can function as a high-level protection promoting defense in depth against unwanted and potentially harmful cyber intrusion, while sophisticated tools and practices can be developed and incorporated into legacy and new control systems to quickly and continuously predict new, identify and isolate existing threats.

[oman] Oman P., Schweitzer E., and Frincke D.: Concerns about intrusions into remotely accessible substation controllers and SCADA systems, Schweitzer Eng. Labs, http://www.selinc.com/techpprs/6111.pdf, 2000

7.11 Communication Network System Requirements

7.11.1 Home Area Network Requirements Framework

Home Area Networks and other local networks need to meet certain requirements in order to properly enable smart metering, energy saving, demand response and smart grid applications. The following requirements are typically mentioned:

- based on open standard interfaces
- supported by a reliable certification process that guarantees interoperability
- layered architecture (ISO/OSI 7-layer model) that enables use of multiple transport, media access and physical layer technologies with the same application layers and network management tools
- secure two way communication
- supports both direct load control and price control
- direct immediate access to nearly real time consumption data
- enables future applications and services that use metered data
- supports embedded generation and detailed end use metering
- supports multi-utility metering.

The service model of the energy conservation service has been described in Figure 1.

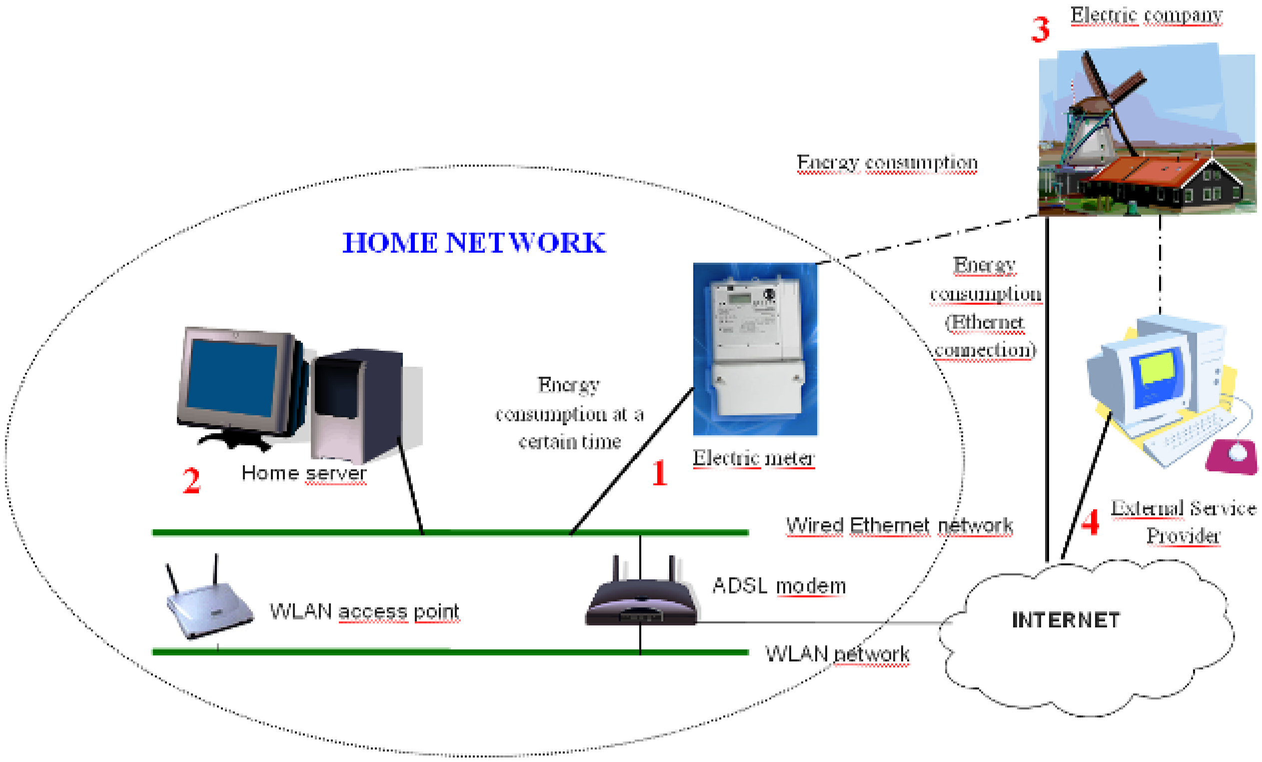


Figure 1. A service model for the energy conservation service.

The key elements of the service are:

An electric meter equipped with an Ethernet or/and (optional) GPRS device and connection for transferring the energy consumption information to the electric company at a certain period.

A home server that works as the central information database concerning household devices and services. More detailed energy consumption information (how much energy at a certain time) is transferred to the home server database that also contains information on the different household electronic devices.

The electric company that provides the core service (electricity) and charges the customer periodically according to consumption.

The external service provider that collects detailed information on household energy consumption and provides a value-added service by analysing the data and providing the customer with suggestions on energy conservation.

Home energy/electricity management has two primary goals:

Design a home energy monitoring infrastructure to provide better means to monitor individual device energy consumption and provision of adequate feedback for the domestic user. The system should also facilitate controlling the devices i.e. switching devices on and off or adjusting thermostats, e.g. the set point for room temperature.

D4.1.4.1: Collection of Smart Grid communication requirements

Promote interoperability between energy producers and home energy consumers. This could mean making pricing information available for the users to guide in starting the washing machine, activating heat storage elements, dropping off devices or controlling thermostats during high network load.

Although there have been several attempts to build the infrastructure for ambient intelligence home environments, none has been a commercial success. There are several boundary conditions to meet before success with such a system:

Introduction of devices to infrastructure should be trivial.

The use of the system and components should be trivial.

When bought in the infrastructure each component should provide immediate benefit for the user, regardless of other available devices

There are clear stakeholders for each component introduced, with a feasible business model. Thus a central server should be avoided, unless there is clear a stakeholder

Touching paradigm should be supported in configuring the system and also interacting with the system

The communication infrastructure should system incremental it should form an communication infrastructure, supported by standards and existing home infrastructures

7.11.2 Communications Interfaces and Interoperability Requirements Framework

In addition to the problem that too many protocols are applied, the fact that proprietary protocols are typically offered for the communication between the meter and the customer is a problem at the moment. Very likely several standards will be applied also in the future for communication between the meter and the customer's systems and appliances although there are many candidates for the common open communication standard. The use of proprietary protocols and the number of alternative standards are expected to reduce rather much. For example, ZigBee Alliance (www.zigbee.org) and HomePlug Powerline Alliance (www.homeplug.org) now develop together their Smart Energy Profile, while use cases are taken from Utility AMI 2008 OpenHAN, Southern California Edison, Texas PUC, and ZigBee Alliance Smart Energy Profile 1.0. While the following communications technologies are found in local networks at the customers, these give a brief overview of communication technologies in local networks.

Euridis bus (IEC 62056-31 standard) over twisted pair

M-bus (Meter bus), (EN 13757 Series standards) over twisted pair or radio, http://www.m-bus.com

D-bus (Dialogue bus) for large facilities

Ibus EIB (ABB)

ModBus over serial line and ModBus/TCP over TCP/IP, http://en.wikipedia.org/wiki/Modbus

EIA-485 over twisted pair with standard or proprietary protocols

Echelon LonWorks (ANSI/CEA-709.1; EN 14908; ISO/IEC 14908 Parts 1, 2, 3, and 4) works on powerline carrier, twisted pair, radio and IP-tunnelling.

HomePlug over powerline comprising HomePlug AV (200 Mbps at 2–28 MHz), HomePlug 1.0 (14Mbps at 4.5–21 MHz) and HomePlug Command&Control (5 kbps, using different frequency bands in USA, Europe, and Asia due to compatibility with local frequency band allocation)

CEBus (EIA-600), powerline (at 100–400 kHz), twisted pair, coax, infrared, RF, and fiber optics

X-10 over powerline

KNX (EN 50090, ISO/IEC 14543) over twisted pair, powerline, RF, infrared, Ethernet)

Ethernet.

While several competing specifications are mentioned, power line communication is discussed in http://en.wikipedia.org/wiki/Power_line_communication. The CENELEC standard EN 50065-1 "Signalling on low-voltage electrical installations in the frequency range 3 kHz to 148.5 kHz" specifies the following four different frequency bands, and it also specifies the maximum output level as a function of frequency.

Band (3–95 kHz) for power companies

Band (95–125 kHz) for all applications

Band (125–140 kHz) for home network systems with a mandatory CSMA/CA access protocol

Band (140–148.5 kHz for alarm and security systems.

The allocation of frequency bands is different in North America and Asia, so a technology originating outside Europe may not meet the European requirements. Also UHF low power radio technologies operating in the 433(Asia)/868(Europe)/915(US) MHz and 2.4 GHz license free ISM-bands are appropriate for communication with the meters, while both open standards and proprietary protocols exist, such as:

ZigBee (Based on IEEE 802.15.4), mesh network, 2.4 GHz, currently the most potential RF protocol

Wireless M-Bus (EN 13757-4)

Z-Wave (proprietary), mesh network, in Europe 868.42MHz

Bluetooth (IEEE 802.15.1), point-to-point, 2.4 GHz, frequency hopping

Wavenis (proprietary), tree, star or mesh topology

INSTEON (proprietary), mesh topology, 902–924 MHz

Plextek Ultra Narrow Band (proprietary)

Everblu (proprietary)

DASH7 (ISO-18000-7), mesh topology, 433 MHz worldwide, ultra low power, range 2 km.

IEEE 802.15.4 WPAN (Wireless Personal Area Network) is the basis for upper layer specifications such as ZigBee, 6loWPAN, WirelessHART or MiWi. These specifications attempt to offer a complete networking solution by developing the upper layers that are not covered by the IEEE 802.15.4 standard. The WPAN as such supports star and point-to-point topologies. WiFi/WLAN based on IEEE 802.11 operating in the 2.4 GHz or 5 GHz band is in some systems used for communication between the meter and the concentrator connected to WAN. Also RFID-like (e.g. inductive 135 kHz or 13.56 MHz) readers limited to close proximity, inductive couplers with IEC 62056-31 EURIDIS, infrared communication and twisted pairs are applied in local meter reading.

The same meter can be expected in the future to communicate with several RF technologies. Smart meter communication modems are already available for smart meter manufacturers that can communicate with GPRS, ZigBee and wireless M-Bus. Both radio transmissions and power line communication technologies have been used for a long time for fast and reliable broadcasting of control signals over wide areas. Many old power line broadcasting systems are being removed now as the smart metering rollouts proceed.

In Germany (129,1 kHz and 139 kHz), Hungary (135,6 kHz) and Czech Republic and Slovakia, European Radio Ripple control system is presently used, while deployment is planned in other countries too. In addition to load control, it can be used also for customer tariff switching, broadcasting information to customers, and regional alarming. Being unidirectional, it cannot replace two way communication technologies, but can complement them by providing fast broadcast of control commands and tariff changes. The data rate is rather limited, because it operates on VLF bands, i.e. the range of a single transmitter typically covers a radius of 300– 500 km.

[reference for this above section]
Pekka Koponen, Marja-Leena Pykälä, Janne Peltonen & Pasi Ahonen. Interfaces of consumption metering infrastructures with the energy consumers. Review of standards [Energiankäyttäjien ja kulutusmittausjärjestelmien väliset tiedonsiirtorajapinnat. Katsaus standardeihin]. Espoo 2010. VTT Tiedotteita – Research Notes 2542. 105 p.

7.11.3 M2M Communication Requirements in Smart Metering

Finnish electric utility companies Vattenfall and Fortum have begun installing GPRS based AMR (Automated Meter Reading) devices at homes, providing means to measure the hourly electricity consumption. This provides means to dynamic pricing of electricity. The AMR solution also provides two way communication, facilitating transmitting real time information (e.g. energy pricing) to consumers. If an infrastructure to measure and control electric devices at home would exist, it would also facilitate a better interplay between electricity consumers and producers. The AMR unit for the first time also provides a central gateway to home, with a clear stakeholder. It is to be expected that a Bluetooth equipped mobile phone may be a generic UI or a remote controller for home appliances in the future.

The networking infrastructure of control systems at home are currently based on Wireless short-range radio (Bluetooth, ZigBee, Z-wave, Insteon or Chirp), or existing cable or power-line infrastructure (X10), or a mixture of both (LonWorks, Insteon, Konnex - KNX) solutions. Ethernet and WLAN based IP solutions e.g. UPnP may be used, together with 3G mobile phones with Bluetooth or WLAN access points. WLAN is however expensive for simple devices and overkill for control purposes. Also several Zigbee based energy monitoring related networking solutions already exist. So to avoid installing GRS/GPRS module to each AMR in apartment complexes, the GPRS based energy AMR device is surrounded by Zigbee equipped AMR infrastructure that can be read through the central node.

Zigbee (/MICAz) based solutions.

In Zigbee based solution, Zigbee is integrated in SmartSocket, SmartPlug, or EnergyAware appliance. In Zigbee there are three types of devices. *Coordinator* is the root device for a network. There is only one root device per network and it usually also acts as a gateway to other networks. Zigbee router acts as an immediate device, passing data from other devices. The SmartSocket, SmartPlug and EnergyAware Appliances might serve as router devices. Zigbee End Device contains the least functionality and can talk only to its parent device, either router or coordinator. This also requires the least amount of energy. Typically a wall switch mount with an access to relay might be implemented by Zigbee End Device. In Zigbee based solutions the coordinator might be embedded in AMR or any other bridge or gateway to other networks. Using mobile phone as a interaction device is limited to interacting with the gateway via Bluetooth or WLAN. If AMR remote control is used it may provide access to the energy aware devices via GPRS.

Wired NFC based solutions.

The problem perhaps is the mobile phone interaction with the system. Each Smart Module would be readable by the touch of the mobile phone. Moreover, the “NFC tag” should be physically situated in a well reachable location in the electric appliance.

Bluetooth/Wibree based mobile phone centric solution

Ideally thinking, an energy aware device (refrigerator, lamp, a radiator with thermostat) should be accessible with the mobile phone. The device should support wireless local short range access and touching. At the same time it should also be capable of being part of the infrastructure for home network. A smart module supporting NFC and Bluetooth may be suggested. Bluetooth scatternets as backbone for home control network backbone have been suggested Source /8/ , but lack standardization. If low power Wibree becomes a market success a scatternet based on Bluetooth/Wibree might be reality? This facilitates both local short range RF interaction with mobile phone and home infrastructure networking.

The system architecture consists of some of the following components:

SmartEnergyModule contains electricity meter, relay functionality, (possibly thermostat and “dimmer” functionality) and a wired or wireless communication protocol radio module. Ideally the radio module should serve both as home networking backbone, and short-range radio communication protocol between the *Smart Energy Module* and user terminal i.e. mobile phone. The module may contain NFC interface for touchMe paradigm.

The smart energy module should physically be inserted into:
a) **Smart Socket** inserted within wall socket or between wall socket, and electric plug (Huovila & al)
b) **Smart Plug** i.e. the power plug, or cord (Seppä –integral part, Strömmer –on the wire) or the transformer unit of the device
c) embedded into the device forming an *energy-aware appliance*

A mobile terminal (Nokia 6131 nfc?) to control or monitor directly the single socket energy expenditure by Physical browsing methods, or locally/remotely via home gateway (see below).

Server or Gateway (e.g. AMR device) that integrates the services of SmartSockets. The gateway provides remote access for the inhabitants or external utility company or both through cellular network or broadband network. The gateway may also provide local access to mobile device via Bluetooth/WLAN. The gateway and home services may also be operated by a telco.

Measurement electronics of the SmartSocket or SmartPlug collect energy consumption from the sensors embedded to the SmartSocket. Every Device is equipped with short-range radio (Bluetooth, ZigBee, Z-wave, Insteon or Chirp) but should support TouchMe type interaction (via NFC, or other means (e.g. ZigBee solution by Huovila &al.).

Gateway can be e.g. an OSGi gateway to broadband network, AMR, or mobile gateway to a cellular network that collects the measurement data from SmartSockets and SmartPlugs and transfers the data to utility company’s or operator’s secure server. The measurement data of each SmartSocket or smartPlug can be accessed with a mobile terminal through broadband internet, cellular network or locally using either short-range radio or NFC equipped terminal.

Ideally consumers should be capable of buying the SmartPlugs or Sockets one by one, being in the beginning capable of communication with them directly with mobile terminal. However, in practice consumers may buy a system from e.g. home automation firm as an integrated package that consists of Socket gateway and reasonable number of SmartSockets.

The price of the SmartSocket system should be reasonable. The customer should be convinced that he/she will save money due to increased energy-awareness. Therefore the price of the SmartSocket system should be at the level that enables him/her to save at least the cost of the monitoring system within the first years of use.

7.11.4 IEC61850-3 environmental standard for power substations

As we move toward the Smart Grid, embedded control and communication become more vital. In addition to the IEC 61850 communication standard, IEC 61850-3 sets ruggedization and environmental standards for networked systems used in power substations.

The IEC 61850-3 standard specifies general requirements for the hardware design of IEC 61850 devices used in substations. IEC 61850-3 devices must meet three major requirements. The three requirements focus on EMI, temperature and shock/vibration resistance.

Electrical substations are severe electromagnetic environments, and various types of disturbances can be easily encountered, as opposed to light industrial or office environments. All electronic equipment installed in the HV electrical substation must be able to resist to electromagnetic phenomena produced in this environment. When selecting networking equipment for use in electrical substations one must be aware of the special requirements imposed by the application.

To overcome this situation, the networking equipment shall be protected against the following hazards:

Conducted and radiated noise: These disturbances are solved by means of shielding and filtering, and are detailed separately in the following section.

Overvoltages: Usually substation power supplies are derived from battery arrays, which may experience overvoltages when charging. Also if the supply is directly obtained from the grid, fluctuations may occur, mainly during disconnections and reconnections in the substation bars. This may easily lead to equipment breakout. To prevent this equipment shall withstand a higher than usual supply voltage range.

Reverse polarity. Every device shall withstand an accidental reversal of the power supply terminals during installation.

Electrostatic discharge: The networking equipment shall be able to work under the presence of electrostatic discharges in exposed metallic parts and interfaces. The devices must not only avoid any damage, but also malfunctioning during the discharges. They occur when electrostatic voltage builds up in humans due to poor electric contact to ground (inadequate shoes) with certain air conditions (lack of air moisture…), and as a result there is big voltage difference between the operator’s exposed body parts and the networking devices, which are usually grounded.

Surge protection: Ground faults, switchgear operation, breaker activations… are substation events which originate very intense current flows and discharges. The currents are coupled into any metallic conductor. As a result of this, huge voltages appear in the power supply terminals of every network device or IED. Thus these equipment must include the mechanisms to cope with these surges. Common design practices include voltage spark gaps, X/Y-type safety capacitors, gas discharge tubes, varistors and zener diodes.

Failure mode: Last, but not least, the networking equipment shall be designed to guarantee a benign failure mode. This will guarantee that the failure of a switch's power supply, for instance, will not affect any of the devices powered by the same power rails, or even the primary power supply. In this way the networking device effectively protects the rest of the equipment from its own failure.

It is important to note that every Ethernet link shall be based on fiber optic technology, in order to get rid of all these potentially harmful phenomena since optical communications are immune to electromagnetic noise and can travel longer distances without performance degradation.

The typical temperature range is -40° to 75°C. The wide temperature requirement is important since substation environments can experience temperatures as high as 75°C and as low as -40°C. The wide temperature requirement can be satisfied with an efficient heat dissipation design for extremely hot surroundings, and a warming system when the temperature drops to extremely cold temperatures.

8 Communication Technologies & System Components

This chapter presents main stream communication system technologies. One can categorize the technologies in various ways but division between wireless and wireline is one of fundamental nature. There is no absolutely best solution or technology, but each has their merits and deficiencies.

Beyond the principal technical design of a system one finds proprietary or single vendor specific systems (e.g. PLC modem or RF mesh) and fully standardized globally standardized ones (ADSL modems, 2G/3G/4G cellular networks).

Table 1: Comparison of Radio Access Technologies

Standard	Family	Primary use	RTT	Downlink	Uplink
LTE	3.9G UMTS (NGMN)	cellular	10 ms	100 Mbps	50 Mbps
802.16e	Mobile WiMAX	Mobile Internet	30 – 50 ms	512 kbps – 1,5 Mbps	512 kbps – 1,5 Mbps

Flash-OFDM	Flash-OFDM	Mobile Internet	< 50 ms	1 Mbps	300 – 500 kbps
802.11	Wi-Fi	Mobile Internet	-	300 kbps – 2Mbps	300 kbps – 2Mbps
CDMA450	CDMA	cellular	< 50 ms	630 kbps – 1,05 Mbps	80 – 500 kbps
EGDE	GSM	cellular	< 150 m	60 – 100 kbps	60 – 100 kbps
HSDPA	UMTS	cellular	50 -150 ms	300 kbps – 1 Mbps	80 – 500 kbps

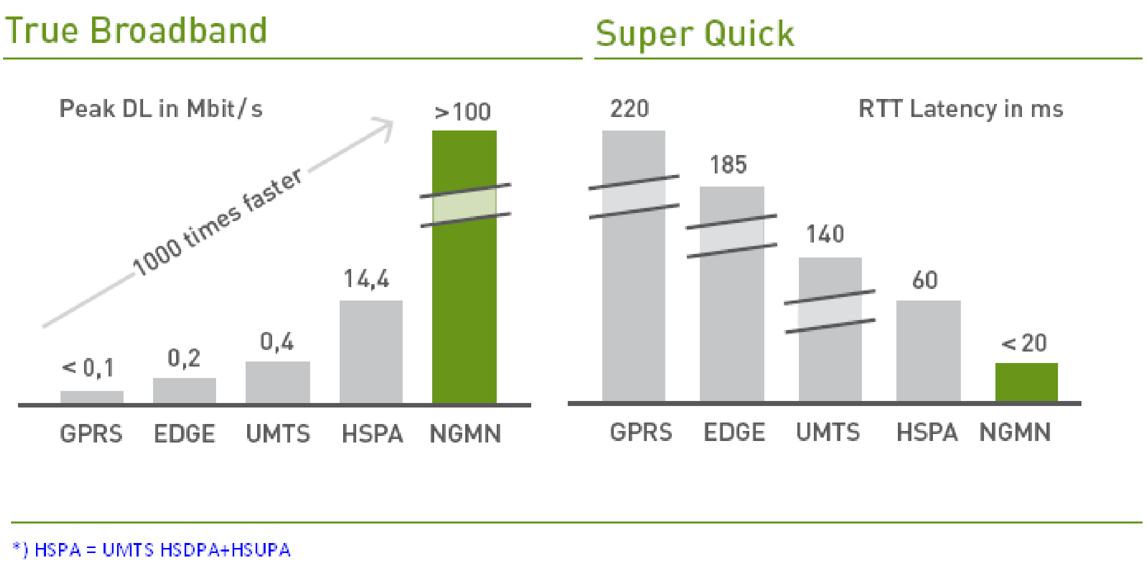


Figure 3: Performance evaluation of different technologies based on NGMN Alliance [**www.ngmn.org**].

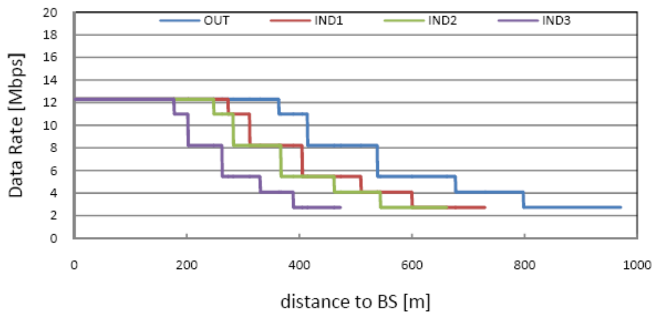
8.1 Mobile broadband (GSM/EDGE, CDMA, WCDMA, WiMax, LTE)

The primary wireless communication subsystem should be based on cost-efficient technology like WiMAX and later LTE (Tier 2 in Figure 2) supporting high data rate mobile communications also in Non-Line of Sight situations. According to latest market development, WiMAX or MobileWiMAX are not necessarily popular technologies of the future, because LTE is expected to assimilate WiMAX. Furthermore, based on available field measurements and literature surveys, the performance of

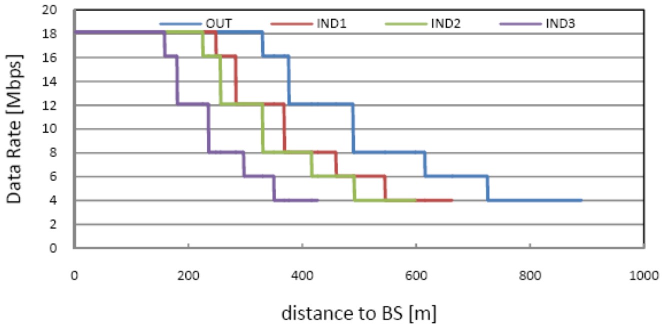
Mobile WiMAX is not as good as anticipated. The measurements and surveys indicate that the actual data rates to uplink direction are 2 - 4 Mbps at 1 km distance, but this depends also on the used frequency bandwidth for the WiMAX connections. The graphs below show examples of estimated data rates in indoor and outdoor environments. The blue curve, labeled as OUT, presents the outdoor case with 7 MHz and 10 MHz bandwidths respectively. The stair-case shape is merely due to the change of the modulation technique. Mobile-WiMAX operates on 2.4GHz, 3.5 GHz and 5.8 GHz frequency bands. Regardless of the chosen frequency band, building a WiMAX test-bed obviously requires support from the vendor provider.

	Modulation	Data Rate [Mbps]
5 MHz	QPSK ½	2.016
	QPSK ¾	3.024
	16 –QAM ½	4.032
	16–QAM ¾	6.048
	64–QAM 2/3	8.064
	64–QAM ¾	9.072
10 MHz	QPSK ½	4.032
	QPSK ¾	6.048
	16 –QAM ½	8.064
	16–QAM ¾	12.096
	64–QAM 2/3	16.128
	64–QAM ¾	18.144
7 MHz	QPSK ½	2.736
	QPSK ¾	4.104
	16 –QAM ½	5.472
	16–QAM ¾	8.208
	64–QAM 2/3	10.994
	64–QAM ¾	12.312

Modulation technique and corresponding data rates



Suburban environment (7 MHz bandwidth)



Suburban environment (10 MHz bandwidth)

Figure 4: Analysis of mobile WiMAX performance at 5, 7, 10 MHz bandwidth.
[J. P. Eira, A. J. Rodrigues, “Analysis of WiMAX data rate performance” Technical University of Lisbon, http://www.anacom.pt/streaming/Analysis_WiMAX.pdf?categoryId=260643&contentId=542756&field=ATTACHED_FILE]

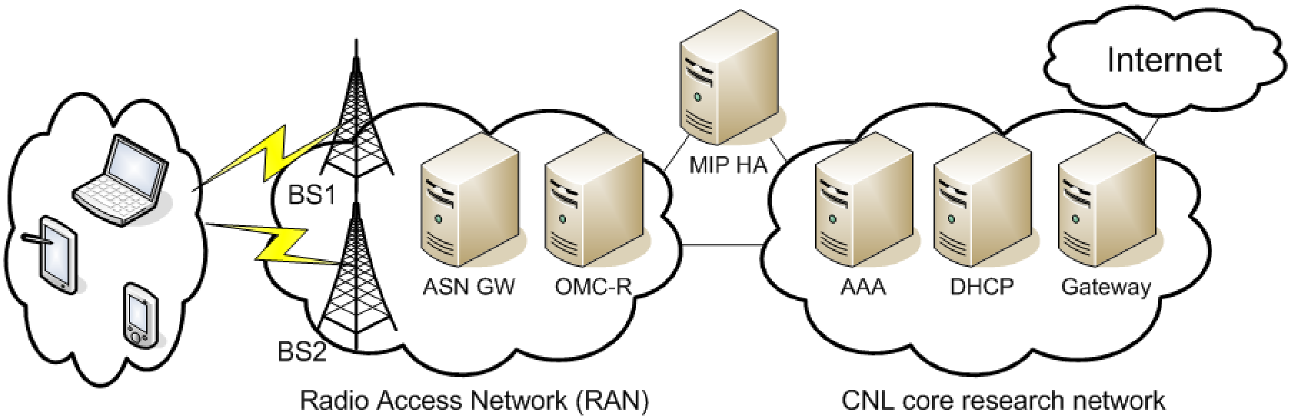


Figure 5: A system diagram of VTT's Mobile WiMAX testbed.

One possibility is to use WLANs to cover especially the critical or problematic "hotspots" in the terrain as may be due to shadow areas. These "hotspots" should be defined according to coverage and capacity requirements. Although WLANs can provide data rates well above 30 Mbps in Line-of-Sight cases, it is important to note that the data rate drops drastically when the terminal is moving away from the AP. The modulation technique can be changed as it is done in mobile-WiMAX case as the radio channel conditions get worse. This significantly lowers the experienced data rates. The diagram below illustrates this.

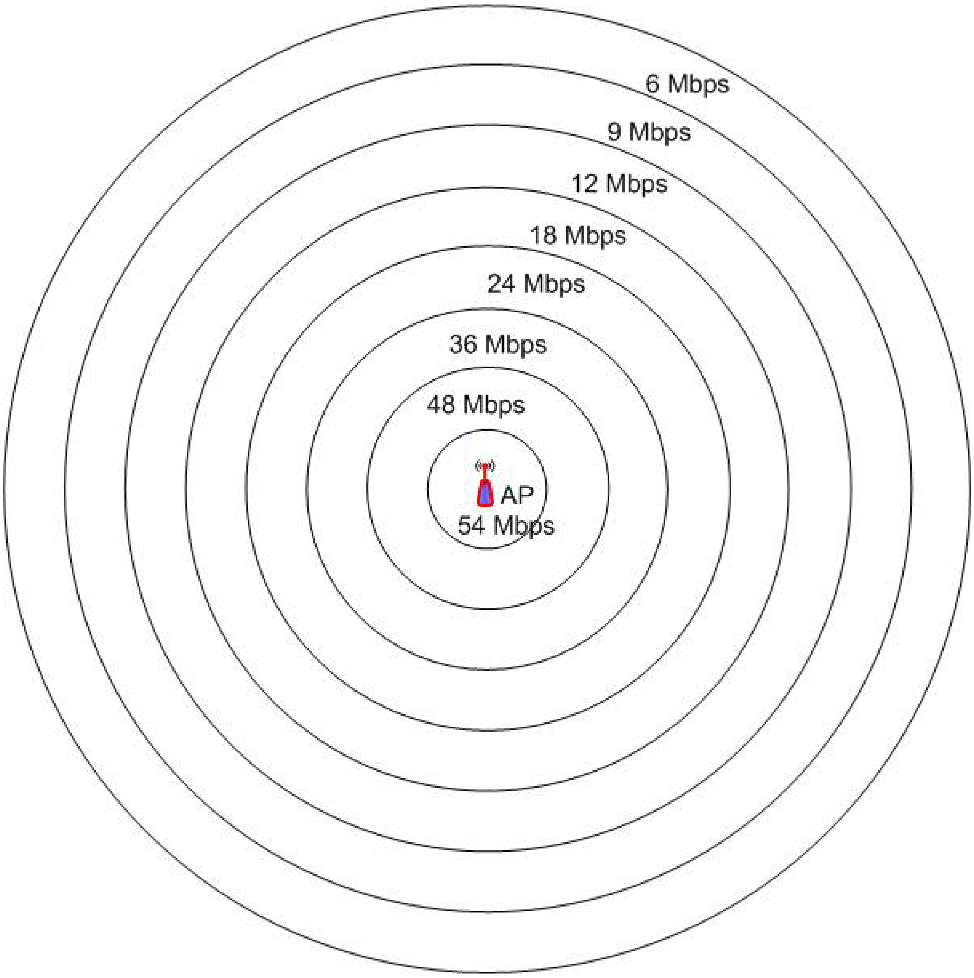


Figure 6. Effects of the distance to experienced data rates when using 802.11g.

The drawback of using WLAN is that the coverage area is small (radius < 200 m), so the whole target site cannot be covered with them. The small coverage area is also problematic when the user is possibly moving fast. The transmission delays in WLAN network can be considered insignificant, but the handover between APs will take approximately 100 – 300 ms, which may cause some unwanted delays e.g. to real-time video streaming. The handover between WLAN and another system will take even longer. This vertical handover is not well supported by COTS products and therefore additional work must be allocated to this functionality if the vertical handover is planned to be supported.

Another option is to utilize WLAN base stations with amplifiers for further coverage, but the use of amplifiers likely requires respective official permits or licenses as well. Anyways, setting additional WLAN base stations could also be considered according to the needed range. The coverage of WLAN can be extended and interference can be reduced also by choosing suitable antenna solutions (e.g. directional antennas, MIMO). Moreover, by tuning the used transmission powers, the interference can be minimized and the capacity can be more evenly distributed among the APs.

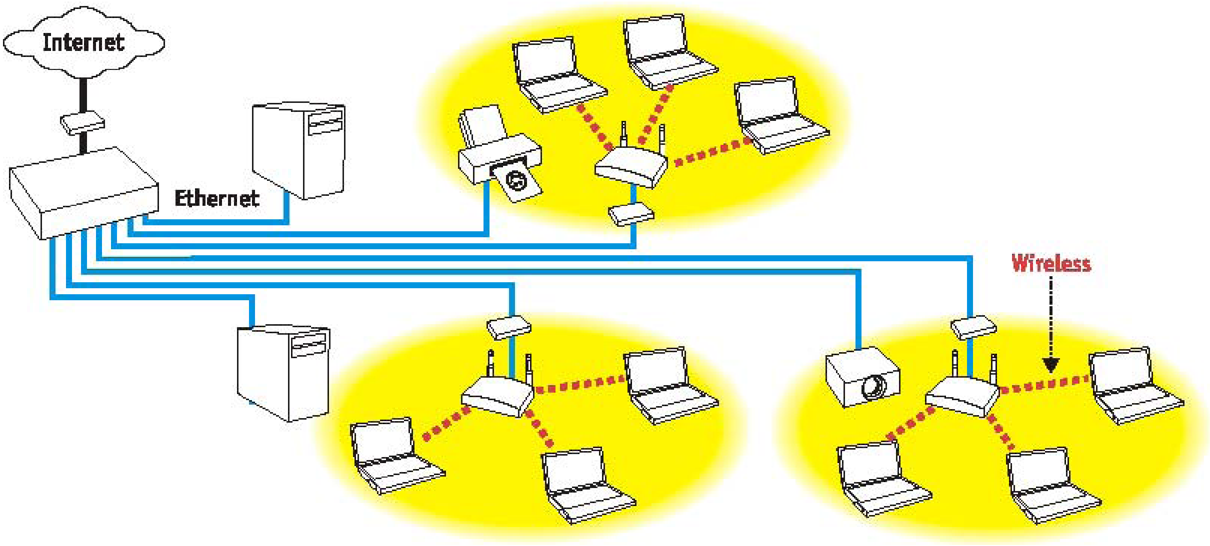


Figure 7: Example of typical WLAN topology.
[http://www.wiborne.com/techpubs/Mesh_deployment_with_WAP.pdf]

One solution to reduce the number of APs is to use long range Outdoor Wireless Access Points e.g. WAP-240 (www.wiborne.com). This access point is designed for point-to-point or point-to-multipoint applications. The AP has three wireless interfaces for sectors or a backhaul. The throughput can be increased using Super G and Turbo modes. For secure data transfer, WEP, WPA, WPA2 encryptions are supported. Layer 2 Mesh, WDS and spanning tree bridging are also supported to data transfers over long distances (up to 145 miles). QoS with video priority is available. Possibilities for mesh deployment are discussed in [www.wiborne.com/techpubs/Mesh_deployment_with_WAP.pdf].

CDMA450

CDMA450 uses code division multiplexing (CDM) so each base station can transmit information simultaneously and at the same frequency. This technology was found suitable for replacing the old analog NMT450. Flash-OFDM at 450MHz and CDMA at 450MHz are already successfully provided by service providers for internet access in rural areas around Europe. The usage of CDMA-technology in Europe is illustrated in the figure below, e.g. CDMA450 is in commercial use in Poland by TP. The CDMA 1xEVDO (Evolution Data Optimized) adds capabilities of high speed data services to CDMA2000 by devoting a second pair of channels for packet switched data transmission. The Revision A is offering higher speeds (3.1 Mbps for downlink and 1.8 Mbps for uplink).

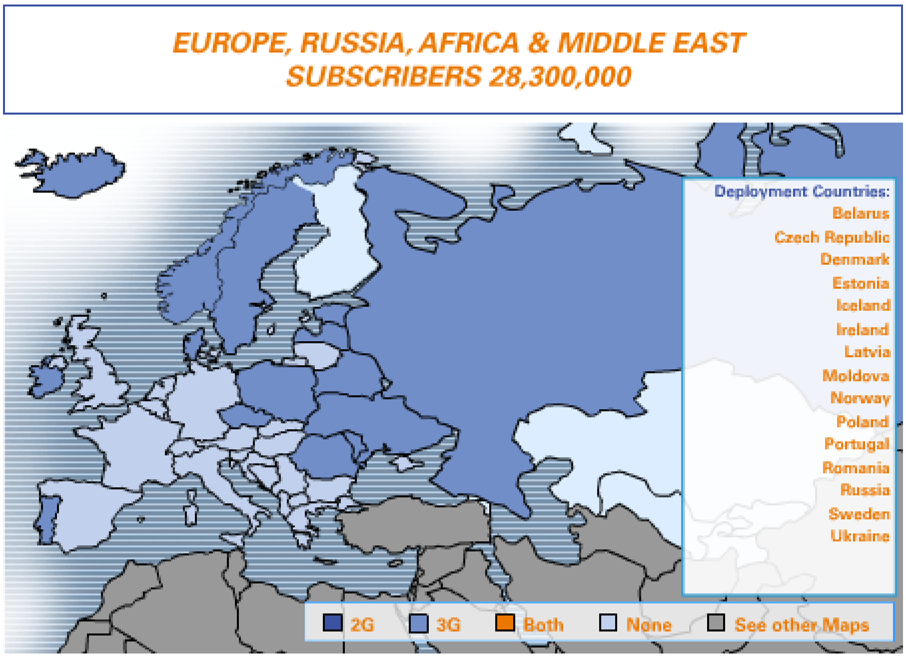


Figure 8: CDMA deployment in Europe.
[http://www.cdg.org/worldwide/index.asp?h_area=2&h_country=36&h_technology=999]

The main advantages of using 450MHz are its propagation characteristics and better penetration compared to commonly used frequencies (800/900/1800/1900MHz), leading to longer ranges. The coverage area of a CDMA450 base station is very large (up to to 50 km) [S. Nedevschi, S. Surana "Potential of CDMA450 for Rural Network Connectivity"]. In Finland, Flash-OFDM @450MHz was selected as a technology to provide wireless broadband data connections in sparsely populated areas. Its maximum data rate in downlink is 2.7 Mbps and uplink 780 kbps. However, the measured average data rates are closer to 1 Mbps and 520 kbps respectively. Being a comparable technology and using the same carrier frequency, the figures give a rough estimate of what CDMA450 performance could be. It is evident that high resolution video streaming (1 Mbps) is not possible with CDMA450. In comparison to e.g. Mobile WiMAX, however, the significant advantage is that the data rate does not drop as drastically when moving away from the base station or when the user is shadowed.

Clearly, a more uniform availability of throughput capacity contributes to robustness, which is a strict requirement for practical security sensitive applications. The guaranteed bandwidth provided with both the above 450 MHz technologies is typically limited below 2 Mbps per one base station.

Flash-OFDM

Digita, a Finnish service provider, has built a mobile broadband network based on Flash-OFDM @ 450MHz technology. This network provides ubiquitous 1- 2 Mbit/s coverage throughout the country. However, Digita has decided to get rid of the business due to lower than expected customer growth and obsolete technology, resulting troubles in maintenance and terminal availability on longer run. Regardless of this decision the network service is supposed to be available still years in the future.

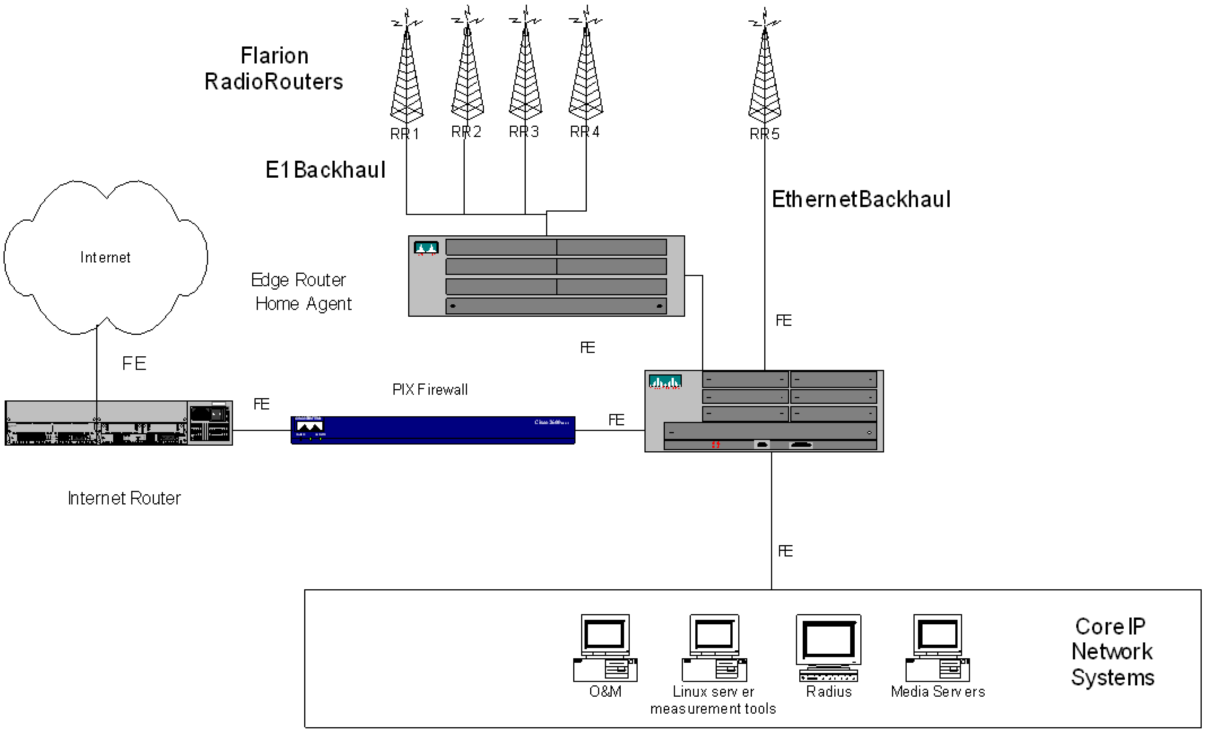


Figure 10: A system diagram of NSN's trial deployment.
[Digita Flash-OFDM Trial System Description document]

GSM/EDGE and UMTS/HSPA

GSM and UMTS are often considered as old technologies, but they are mainstream, available and still being developed further. Network reliability and robustness have been proven over the years.

One solution to enhance the future availability is to use existing GSM/UMTS infrastructure and available multi-band and multi-system modems. For example, two versions of the COM-1289 are available from Eurotech, i.e. one with a 4-band 3G HSDPA/UMTS modem with GPRS/GSM support and one with a Dual band (800/1900 MHz) CDMA 1XEV-DO Rev A 3G modem. For this mode, high peak data rates are claimed to be 3.6Mbps in HSDPA/UMTS networks, 216kbps in EDGE/GPRS/GSM networks, and up to 3.1Mbps using CDMA EV-DO Rev A. The average data rates can be expected to be significantly lower.

Another very interesting product is the rugged Wireless and Mobile Access Router DuraMAR2200 (see http://www.eurotech.fi/products/duramar2000.html), which has integrated HSDPA, CDMA, GPRS, WiMAX and GPS support. This compact size is an accomplishment manifesting true ingeniousness in both engineering and craftsmanship.

For the backup communication system, another highly secure solution would be to utilize TETRA (Terrestrial Trunked RAdio), which is specifically designed for use by government authorities, emergency services, (police, fire departments and research and rescue) and the military. Due to the low level of current penetration of TETRA, however, the respective available equipment are relatively expensive and do not feature the latest advances in technology. TETRA has some features that should be considered in SGEM use cases. It supports very fast call setup time, which typically is less than 250 ms. The system works at high speeds (> 400 km/h) and provides support for both air-interface encryption and end-to-end encryption.

LTE and LTE-Advanced

LTE (Long Term Evolution) is a 3GPP standard that has been optimized for packet switched networks only, and it's the latest standard in the mobile network technology tree that previously realized the GSM/EDGE and UMTS/HSxPA network technologies. LTE is a set of enhancements to the Universal Mobile Telecommunications System (UMTS) that was introduced in 3rd Generation Partnership Project (3GPP) Release 8. The viewpoint of e.g. Next Generation Mobile Networks Alliance (NGMN) is that next generation networks are based upon Internet Protocol (IP), while 3GPP has done feasibility studies into All IP Networks (AIPN). Proposals developed included recommendations for 3GPP Release 7, which are the foundation of higher level protocols such as LTE. These recommendations are part of the 3GPP System Architecture Evolution (SAE). Accordingly, 3GPP Release 8 focuses on adopting 4G mobile communication's technology including an all-IP flat networking architecture. Part of the LTE standard is the System Architecture Evolution, a flat IP-based network architecture designed to replace the GPRS Core Network and ensure support for, and mobility between, some legacy or non-3GPP systems, for example GPRS and WiMAX respectively.

E-UTRAN is the air interface of LTE, and the LTE specification provides downlink peak rates of at least 100 Mbit/s, an uplink of at least 50 Mbit/s and RAN round-trip times of less than 10 ms. LTE supports scalable carrier bandwidths, from 1.4 MHz to 20 MHz and supports both Frequency Division Duplexing (FDD) and Time Division Duplexing (TDD). The main advantages with LTE are high throughput, low latency, plug and play, FDD and TDD in the same platform, an improved end-user experience and a simple architecture resulting in low operating costs. LTE will also support seamless passing to cell towers with older network technology such as GSM, cdmaOne, UMTS, and CDMA2000. Despite initial development of the rival UMB standard, which was designed as an upgrade path for CDMA networks, most operators of networks based upon the latter system have also announced their intent to migrate to LTE, resulting in discontinuation of UMB development.

A large amount of the work is aimed at simplifying the architecture of the system, as it transits from the existing UMTS circuit + packet switching combined network, to an all-IP flat architecture system. The pre-4G standard is a step towards LTE Advanced, a 4th generation standard (4G) of radio technologies designed to increase the capacity and speed of mobile telephone networks. Indeed, the next step for LTE evolution is LTE Advanced, which is a preliminary mobile communication standard, formally submitted as a candidate 4G system to ITU-T and expected to be finalized in 2011. It is standardized in 3GPP Release 10 as a major enhancement of the 4G.

3GPP Long Term Evolution (LTE) standard. LTE Advanced is backwards compatible with LTE and uses the same frequency bands, while LTE is not backwards compatible with 3G systems. The importance and timeframe of LTE Advanced will of course largely depend on the success of LTE itself. LTE Advanced will be fully built on the existing LTE specification Release 10 and not be defined as a new specification series. So, if possible, LTE-Advanced will be a software upgrade for LTE networks.

In addition to very high data rates, LTE-A also targets faster switching between power states and improved performance at the cell edge. One of the important LTE Advanced benefits is the ability to leverage advanced topology networks; optimized heterogeneous networks with a mix of macros with low power nodes such as picocells, femtocells and new relay nodes. The next significant performance leap in wireless networks will come from leveraging topology and brings the network closer to the user by adding many of these low power nodes. Thereby, LTE Advanced further improves the capacity and coverage, and ensures user fairness. LTE Advanced also introduces multicarrier to be able to leverage ultra wide bandwidth, up to 100 MHz of spectrum supporting peak data rates up to 1 Gbit/s.

8.2 Copper, Cable-TV, Fiber

8.2.1 Copper / Digital Subscriber Line

Digital Subscriber Line (**DSL**) is a family of technologies that provides digital data transmission over the wires of a local telephone network. DSL originally stood for *digital subscriber loop*.
In telecommunications marketing, the term Digital Subscriber Line is widely understood to mean Asymmetric Digital Subscriber Line (ADSL), the most commonly installed technical variety of DSL. ADSL service is typically delivered simultaneously with regular telephone on the same telephone line. This is possible because ADSL uses a higher frequency. These frequency bands are subsequently separated by filtering.

ADSL technologies typically achieved maximum downstream data rates of 8 Mbps (ADSL) to 24 Mbps (ADSL2+) and upstream 1 Mbps. Data throughput also depends on line condition, length and service-implementation.

Unlike with Symmetric-High-Data-Rate Digital Subscriber Line (SHDSL), with ADSL, POTS service can be carried in the lower 4 kHz bandwith.
In ADSL, the data throughput in the upstream direction, (i.e. in the direction to the service provider) is lower, hence the designation of *asymmetric* service.

In Symmetrical High Data Rate Digital Subscriber Line (SHDSL) service, the downstream and upstream data rates are equal.

An extension to even higher frequency utilization (≤30MHz) on the twisted pair, Very-High-Speed Digital Subscriber Line (VDSL2) connections can be used for services like triple play and HDTV. VDSL operates at reliable high bit rates on short loops.

VDSL2 loop may be extended approximately 2.5 km (0.4 mm) in order to use special US0 band (voice frequency band), echo cancellers and time-domain equalizers. VDSL2 as a last mile connection to customer premises with FTTB is a one alternative to provide high speed broadband services using existing twisted pair cabling of the building.

Overview of commonly used DSL technologies:

ADSL, (7 Mbps down, 800 kbps up)
ADSL2, (8 Mbps down, 1 Mbps up)
ADSL2+, (24 Mbps down, 1 Mbps up)
ADSL2-RE, (8 Mbps down, 1 Mbps up)

Extends coverage area of 768 kbps service approximately 37% compared to ADSL.

SHDSL, (192 kbps to 2.312 Mbps, extended mode 5.6 Mbps / 1 pair / down /up)

Used for example in mobile backhaul solution. SHDSL was initially developed to provide equivalent E1/T1 service in more economic way. SHDSL modems may provide E1/T1 and Ethernet or ISDN tributary interfaces.

VDSL2

ITU-T G.993.2 supports typically bidirectional symmetrical data rates (upstream + downstream) up to 50 Mbps each, or asymmetrical data rates up to 100 Mbps downstream and 10 Mbps upstream on twisted pairs. Recommendation is defined to allow the use of up to 17MHz (on twisted pair subscriber line) and 30 MHz (in-house application) of the frequency spectrum.

ADSL and VDSL2 are using so-called Discrete-Multi-Tone (DMT) modulation of individual carriers spaced at app. 4 or 8 kHz, whereas SHDSL uses time-domain modulation, which also reaches into the voice frequency band.

Voice and data

Typically ADSL and VDSL use a second, higher frequency band (greater than 25 kHz) above the low frequency regime (5 kHz and below) used by voice communications. On the customer premises, a DSL filter is installed on each outlet for telephone handsets to remove the high frequency band, eliminating interference with the operation of the telephone set, and enabling simultaneous use.

Typical setup and connection procedures

Physical connection must come first. On the customer side, the DSL Transceiver, or ATU-R, or more commonly known as a DSL modem, is hooked up to a phone line. The telephone company (telco) connects the other end of the line to a DSLAM, which concentrates a large number of individual DSL connections into a single box. The location of the DSLAM depends on the telco, but it cannot be located too far from the user because of attenuation, the loss of data due to the large amount of electrical resistance encountered as the data moves between the DSLAM and the user's DSL modem. It is common for a few residential blocks to be connected to one DSLAM.

When the DSL modem powers up it goes through a sync procedure. The actual process varies from modem to modem but generally involves the following steps:

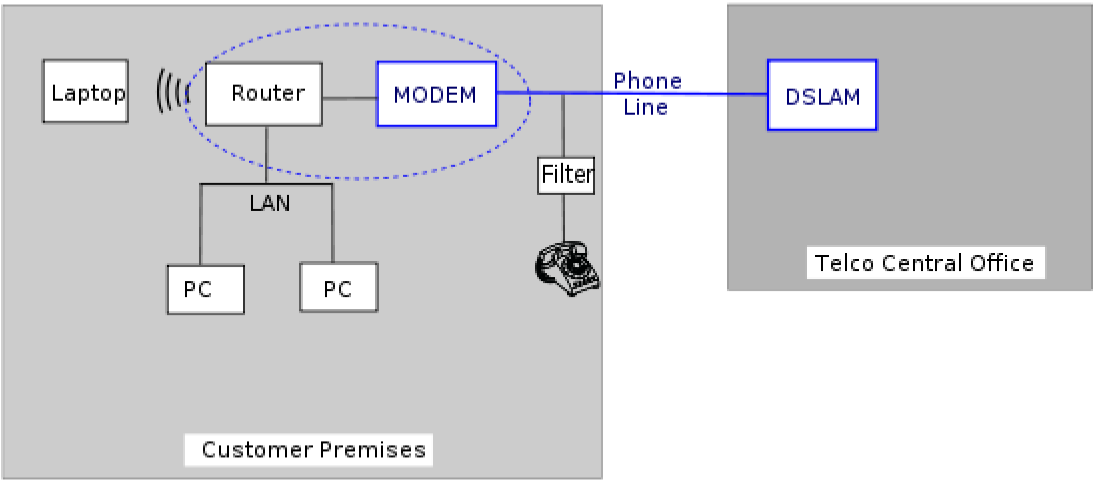
The DSL transceiver performs a self-test.

The DSL transceiver checks the connection between the DSL transceiver and the computer. For residential variations of DSL, this is usually the Ethernet (RJ-45) port or a USB port; in rare models, a FireWire port is used. Older DSL modems sported a native ATM interface (usually, a 25 Mbit serial interface). Also, some variations of DSL (such as SDSL) use synchronous serial connections.

The DSL transceiver then attempts to synchronize with the DSLAM. Data can only come into the computer when the DSLAM and the modem are synchronized. The synchronization process is relatively quick (in the range of seconds) but is very complex, involving extensive tests that allow both sides of the connection to optimize the performance according to the characteristics of the line in use. External, or stand-alone modem units have an indicator labeled "CD", "DSL", or "LINK", which can be used to tell if the modem is synchronized. During synchronization the light flashes; when synchronized, the light stays lit, usually with a green color.

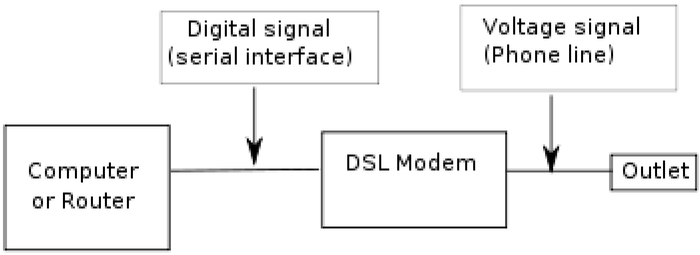
Modern DSL gateways have more functionality and usually go through an initialization procedure very similar to a PC boot up. The system image is loaded from the flas memory; the system boots, synchronizes the DSL connection and establishes the IP connection between the local network and the service provider, using protocols such as DHCP or PPPoE. The system image can usually be updated to correct bugs, or to add new functionality.

The accompanying figure is a schematic of a simple DSL connection. The right side the shows a DSLAM residing in the telco central office. The left side shows the customer premises equipment with an optional router. This router manages a local area network (LAN) off of which are connected some number of PCs. With many service providers, the customer may opt for a modem which contains a wireless router. This option (within the dashed bubble) often simplifies the connection.



Equipment

The customer end of the connection consists of a terminal adaptor or in layman's terms "DSL modem". This converts data between the digital signals used by computers and the voltage signal of a suitable frequency range which is then applied to the phone line.



DSL Modem schematic

In some DSL variations (for example, HDSL), the terminal adapter connects directly to the computer via a serial interface, using protocols such as ethernet or V.35. In other cases (particularly ADSL), it is common for the customer equipment to be integrated with higher level functionality, such as routing, firewalling, or other application-specific hardware and software. In this case, the equipment is referred to as a gateway.

Some kinds of DSL technology require installation of appropriate filters to separate, or "split", the DSL signal from the low frequency voice signal. The separation can take place either at the demarcation point, or with filters installed at the telephone outlets inside the customer premises. Either way has its practical and economical limitations. See ADSL for more information about this.

At the exchange, a digital subscriber line access multiplexer (DSLAM) terminates the DSL circuits and aggregates them, where they are handed off onto other networking transports. In the case of ADSL, the voice component is also separated at this step, either by a filter integrated in the DSLAM or by a specialized filtering equipment installed before it. The DSLAM terminates all connections and recovers the original digital information.

Asymmetric Digital Subscriber Line (**ADSL**) is the common form of the Digital Subscriber Line technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.

A splitter allows a single telephone connection to be used for both ADSL service and voice calls at the same time. ADSL can generally only be distributed over short distances from the central office, typically less than 4 km (2 mi), but has been known to exceed 8 km (5 mi) if the originally laid wire gauge allows for farther distribution.

Data carried by the ADSL are typically routed over the telephone company's data network and eventually reach a conventional Internet Protocol network.

Usually at homes ADSL modem is embedded with WLAN access so that, e.g. lap tops can easily be connected to the network/Internet.

8.2.2 Coaxial cable

Coaxial cable is used as a transmission line for radio frequency signals, in applications such as connecting radio transmitters and receivers with their antennas, computer network (Internet) connections, and distributing cable television signals. One advantage of coax over other types of radio transmission line is that in an ideal coaxial cable the electromagnetic field carrying the signal exists only in the space between the inner and outer conductors. This allows coaxial cable runs to be installed next to metal objects such as gutters without the power losses that occur in other types of transmission lines, and provides protection of the signal from external electromagnetic interference.

Cable-based services

Coaxial cables are capable of bi-directional carriage of signals as well as the transmission of large amounts of data. Cable television signals use only a portion of the bandwidth available over coaxial lines. This leaves plenty of space available for other digital services such as cable internet, cable telephony and wireless services, using both unlicensed and licensed spectrum. Broadband Internet is achieved over coaxial cable by using cable modems to convert the network data into a type of digital signal that can be transferred over coaxial cable.

In North America, Australia and Europe many cable operators have introduced cable telephone service. In many cases, digital cable telephone service is separate from cable modem service being offered by many cable companies and does not rely on IP traffic or the Internet.

Several cable operators have begun offering wireless services to their subscribers. Most notably was the September 2008 launch of Optimum Wi-Fi by Cablevision. Cablevision has reported a double digit reduction in subscriber churn since launching Optimum Wi-Fi, even as Verizon has rolled out FiOS, a competitive residential broadband service in the Cablevision footprint. Other Tier 1 cable operators, including Comcast, have announced trials of a similar service in sections of the US Northeast.

8.2.3 Optical fiber communication

An **optical fiber** is a thin, flexible, transparent fiber that acts as a waveguide, or "light pipe", to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference.

Each fiber can carry many independent channels, each using a different wavelength of light (wavelength-division multiplexing (WDM)). The net data rate (data rate without overhead bytes) per fiber is the per-channel data rate reduced by the FEC overhead, multiplied by the number of channels (usually up to eighty in commercial dense WDM systems as of 2008).

For short distance applications, such as creating a network within an office building, fiber-optic cabling can be used to save space in cable ducts. This is because a single fiber can often carry much more data than many electrical cables, such as 4 pair Cat-5 Ethernet cabling. Fiber is also immune to electrical interference; there is no cross-talk between signals in different cables and no pickup of environmental noise. Non-armored fiber cables do not conduct electricity, which makes fiber a good solution for protecting communications equipment located in high voltage environments such as power generation facilities, or metal communication structures prone to lightning strikes. They can also be used in environments where explosive fumes are present, without danger of ignition. Wiretapping is more difficult compared to electrical connections, and there are concentric dual core fibers that are said to be tap-proof.

The benefits of Fiber optic communications

SPEED: Fiber optic networks operate at high speeds - up into the gigabits

BANDWIDTH: large carrying capacity

DISTANCE: Signals can be transmitted further without needing to be "refreshed" or strengthened.

NOISE IMMUNITY: Greater resistance to electromagnetic noise such as radios, motors or other nearby cables.

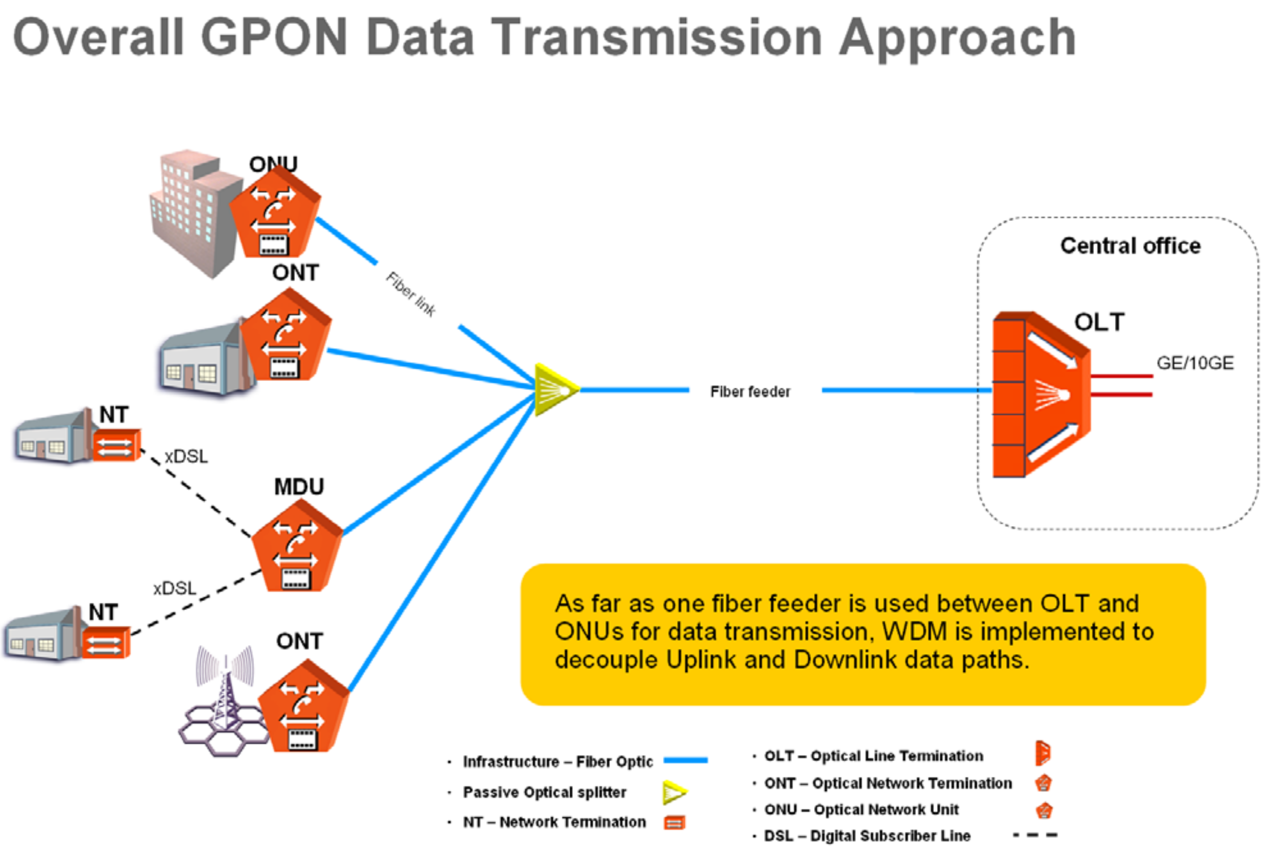
MAINTENANCE: Fiber optic cables costs much less to maintain.

PRACTICAL IMPLEMENTATION for public and private fiber-optic communication are Gigabit-Ethernet switching and transmission systems, operating at typically 1Gbps at low optical module cost. Formerly Synchronous Digital Hierarchy (SDH) systems were widely installed, also in dedicated networks for data transmission and fast power-line protection switching. Typical line rates are quadruples of 155Mbps (622Mbps, 2.4Gbps, 10Gbps).

To increase bandwidth on one fiber, Wavelength Division Multiplexing (WDM) may be used, mainly in the 1.5µm wavelength operating window. From a few up to about 80 different wavelengths may be superimposed from different lasers by an optical combiner and later decomposed by optical filters. Optical amplification may be used in addition to increase reach.

Recently, optical Gigabit Ethernet point to point (P2P) links are used also for residential and enterprise communication purposes, upgrading DSL and 3GPP-radio link speed or replacing SDH based fiber technology.

To further reduce cost in fiber-optic transmission for residential and enterprise communication purposes, Passive Optical Networks (PON) were standardized and introduced in recent years. Typically one fiber is used for uplink and downlink for a large group of customers, by optically splitting one downlink signal from 32 into up to several hundred fibers (Point to Multi-Point – P2MP). The advantage compared to P2P systems is to avoid mechanical handling of up to 5-digit numbers of optical fibers in one concentrator location. In contrast to some kilometer reach of DSL-systems, PON-systems may reach up to several dozen kilometers from concentrator (Optical Line terminal – OLT) to the most distant end-user (Optical Network Termination – ONT).
Please see the diagram below:



Today's Generic-PON (GPON, standardized by ITU/ETSI) systems are using cell-based multiplexing and additional encryption in the downstream link to address and insure privacy of each end-user. Individual upstream channels are multiplexed by time slot assignment into a common signal. Typical total downstream bandwidth is starting from 2.4Gbps (divided by no. of connected users) up to 10Gbps as standard implementation evolves. Total uplink bandwidth is limited to a total of about 1.2Gbps for practical fiber-optic pulse delay reasons.
GPON systems are limited to the utilization of a low number of different WDM downlink channels, as the signals need to be cost-efficiently separated afterwards.
For cost reasons, just one optical upstream wavelength is used.

To overcome intrinsic limitations of time domain-multiplexing disadvantages, new PON approaches are being researched and engineered. So-called Next Generation Optical Access (NGOA) systems will generate hundreds of individually modulated wavelength's downstream signals with very narrow spacing in the optical GHz range, transmitted from one concentrator system.
Optical heterodyne detection and locked wavelength displacement for uplink signal generation, integrated into a single ONT module promise individual Gbps peak transmission speed at affordable cost.

PON systems may be used mainly for Smart Grid communication purposes in the residential and enterprise area, as fiber deployment commences.

8.3 Communication Network Components Available/Applicable to Smart Grids

Several companies are already providing networking products targeting specifically the Smart Grid. The following chapters identify some companies and their respective products.

8.3.1 ThereGate

Therecorporation focuses on energy saving and efficiency, while their solutions are based on the product ThereGate, which was formerly known as the Nokia Home Control Center or HCC. ThereGate is an ideal platform for many different applications and needs, because it is a technology-independent open Linux-based platform that supports the most common smart home technologies. So, they have a wide range of solutions from different vendors to choose from, and also for third parties to create new solutions and applications. ThereGate's hardware platform includes several radio and bus interfaces, while it can easily be expanded with other connectivity options as required for specific applications. See www.therecorporation.com for more information.

Figure 11. ThereGate.

A mobile phone and a web browser are the two most important control nodes in the solution. The ThereGate devices will include monitoring and controlling of energy consumption while also act as devices connected to security and safety sensors, so control of all energy and home solutions is made easy and convenient via a simple unified interface. ThereGate can also be integrated into different back-end systems, internet services and portals. The back-end servers ensure a seamless and secure link between a mobile phone and the ThereGate, while automatic updating of the ThereGate and device software keeps the whole system up-to-date without effort from the customers. Indeed, the value for the end customer comes from the integration of different individual devices and entire systems from 3rd party vendors, all under the control of one user interface, provided by ThereGate.

8.3.2 Viola Systems

Viola System's M2M Solution www.violasystems.com/products/viola_m2m_solution.htm simplifies use of new generation cellular networks (GPRS/EDGE/UMTS) for various data communications purposes, so that there is little need to make changes to the existing systems.

First, the Viola M2M Gateway is installed to the main location to which the remote devices are to be connected. Then, the remote devices are linked to the GPRS network with their "Arctic" products. Finally, after some configuration effort, secured, cellular-based wide area network connectivity is available.

Arctic IEC-104 Gateway makes possible the upgrading of a communication system by enabling protocol conversion from IEC-101 to IEC-104 (and vice versa), so conventional IEC-101 devices can be attached to a modern TCP/IP based IEC-104 control system. The IEC 60870 protocol family is a vendor-independent communication standard for electricity industry. Ethernet, GPRS and EDGE network interfaces provide a seamless communication solution for most of the applications. Secure (Firewall, VPN) and two-way GPRS/EDGE communication (static IP addresses) is provided with Viola M2M Gateway or with mobile operator private APN service.

Figure 14. Arctic 3G Gateway from Viola Systems.

For high bandwidth applications, the above Arctic 3G Gateway provides the possibility to extend the reliability of Viola's traditional GPRS based Industrial solutions to the 3G / HSDPA / UMTS networks.

Figure 15. Arctic RTU from Viola Systems connects remote devices to SCADA.

The above Arctic RTU provides wireless monitoring and control of field devices via GPRS. All field assets can be monitored and controlled seamlessly from a central site. Arctic RTU can be connected to the field devices by using digital IO:s and controlled through 2 serial ports using IEC-104 or Modbus TCP protocols from the SCADA. Arctic RTU is an entry level RTU with integrated communication capability and seamless integration to SCADA.

Figure 17. Arctic AMR from Viola Systems providing communication for smart metering.

The above Arctic AMR is a plug and play device that makes any meter Smart Grid capable. Arctic AMR automatically retrieves all the meter data and transfers to a server. The Utility can use the meter data for e.g. billing, distribution control, avoiding thefts, and improve efficiency.

8.3.3 Cisco

The Cisco 2500 Series Connected Grid Switch is a rugged switch optimized for use in transmission and distribution (T&D) power substations. The Cisco 2520 Connected Grid Switch (CGS 2520) is designed for substation networks to meet the harsh environments common in transmission and distribution substations. The CGS 2520 uses Cisco IOS Software, the operating system that powers millions of Cisco switches worldwide. The primary features include: Rugged industrial design and substation compliance IEC-61850-3 and IEEE 1613 for utility substation environments; No fans, no moving parts for maximum reliability; Tools for easy deployment, management, and replacement; Extensive instrumentation and remote diagnostic capabilities; Advanced Cisco IOS

Software features such as 802.1x, Layer 2-Layer 4 access control lists, port security; Advanced QoS capabilities to support mission-critical substation applications such as supervisory control and data acquisition (SCADA) and IEC 61850 Generic Object-Oriented Substation Events (GOOSE) messaging; Comprehensive network security features based on open standards; Field-replaceable components such as power supplies and Small Form-Factor Pluggables (SFPs); and Intuitive graphical user interface (GUI) using Cisco Configuration Professional.

Figure 19. Cisco 2500 Series Connected Grid Switch.

The rugged CGS 2500 (www.cisco.com/en/US/products/ps10978/index.html) shown above is designed to be used along with the Cisco 2000 Series Connected Grid Router (www.cisco.com/en/US/products/ps10977/index.html) shown below.

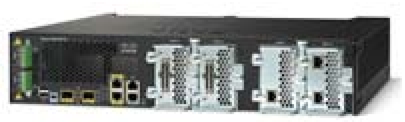


Figure 20. Cisco 2000 Series Connected Grid Router.

The Cisco 2000 Series Connected Grid Router is a rugged router optimized for use in transmission and distribution (T&D) power substations. The Cisco 2010 Connected Grid Router (CGR 2010) is designed for substation networks to meet the harsh environments common in transmission and distribution substations. Cisco IOS software delivers the benefits of integrated security for NERC/CIP compliance, quality of service, and network management to help ensure integrity and priority of operational data communications. The Cisco CGR 2010 router features include: Rugged industrial design and substation compliance with IEC-61850-3 and IEEE 1613 for utility substation environments; Integrated security to help utilities address compliance with critical infrastructure protection mandates; High availability design for optimum network up time and redundancy; Network and device management tools for deployments, upgrades, and remote monitoring; Advanced quality of service (QoS) capabilities to support mission-critical substation communications such as SCADA (Supervisory Control and Data Acquisition), and Comprehensive network security features based on open standards.

8.3.4 Satel

SATEL’s radio modem product SATELLINE (www.satel.com/products/satelline/) plays a central role in Automated Meter Reading, in remote control of electricity distribution, as well as in monitoring Wind Farms. The SATELLINE radio modem product group provides an easy and economic way of setting up a local area data communication network. The applications related to both public and private sectors are countless - hence the SATELLINE has become the most widely known of the SATEL radio modems.

SATELLINE radio modems have a small but important role in providing a compact and reliable means of communication between the disconnector terminal units and the network control centre, as explained in www.satel.com/applications/energy/electricity-distribution/

Also, the SATELLINE radio link supports IEC communication protocol as required for monitoring and controlling wind farms, as explained in www.satel.com/applications/energy/monitoring-wind-farms/ and www.satel.com/applications/energy/wind-mills-with-radios/ where especially a dedicated network with high speed narrow band radiomodems such as SATEL's SATELLINE-3AS is most adequate.

8.3.5 Rugged Com

RuggedCom has developed communications products and technologies specifically designed to operate reliably in harsh environments such as those found in electric utility substations. These products comprise what RuggedCom calls RuggedGRID solution and are designed to create a reliable and rugged communications backbone for the Smart Grid as depicted in www.ruggedcom.com/applications/smart-grid/ and the figure below.

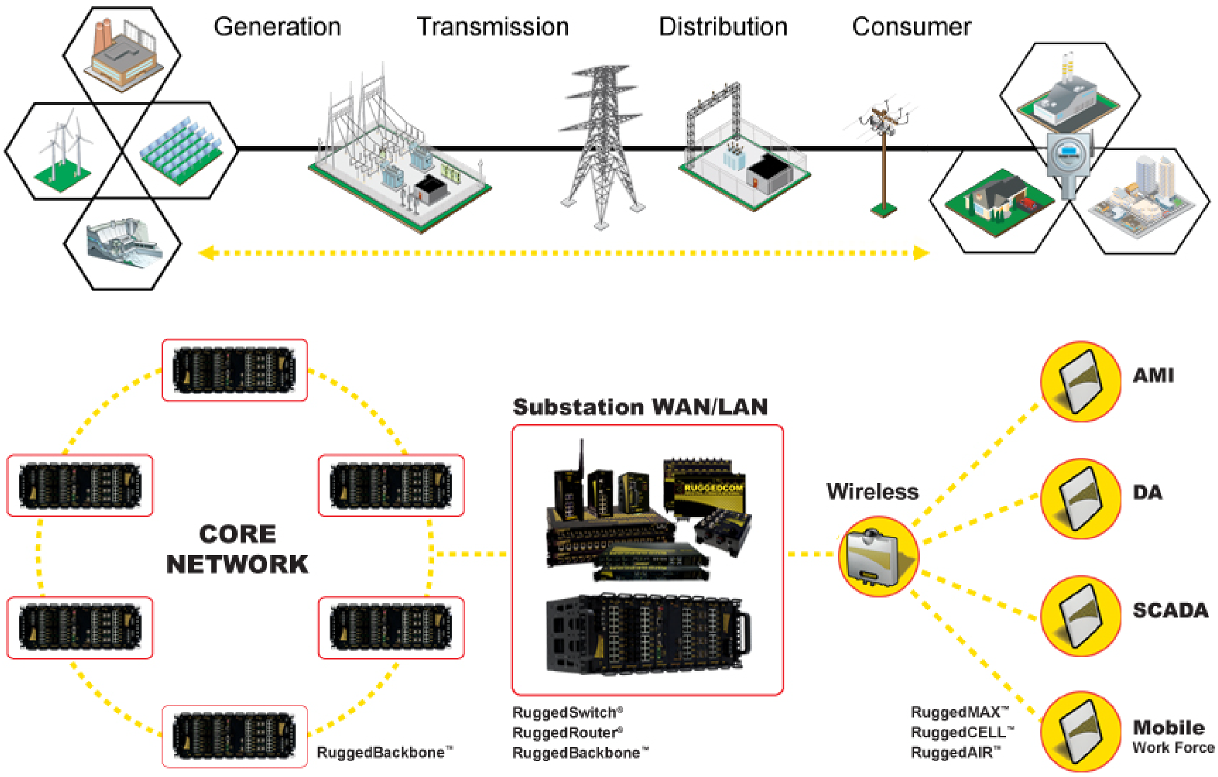


Figure 21. Smart Grid as seen by RuggedCom.

The RuggedBackbone RX5000 is a high port density routing and switching platform, designed to operate in harsh environments. The RuggedBackbone can withstand high levels of electromagnetic interference, radio frequency interference and a wide temperature range of -40°C to +85°C. This platform is designed to meet the challenging climatic and environmental demands found in utility, industrial and military network applications. The RX5000's Rugged hardware design coupled with RuggedCom's embedded operating system provides system reliability, cyber security and networking features making it well suited for creating secure Ethernet networks for mission critical, real-time, control applications. The RX5000 is a scalable, hot-swappable, modular platform which provides its users with the ability to change the RuggedBackbone as their network grows or their needs change.

Figure 22. RuggedBackbone RX5000 from RuggedCom.

The RuggedRouter family of products are industrially hardened with integrated router, firewall, and VPN functionality. The RuggedRouter can be used to establish an electronic security perimeter around critical cyber assets found in control and automation systems, in order to prevent the disruption of operations by accidental or malicious acts. Ideally suited for electric power utilities, the industrial plant floor, and traffic control system applications, the RuggedRouter is designed to protect and secure SCADA system networks connected directly to the Internet, or within a company's private Wide Area Network (WAN) or Local Area Network (LAN).

Figure 23. RuggedRouters from RuggedCom.

The RuggedSwitch family of rugged Ethernet switches are specifically designed to operate reliably in industrially harsh environments. The RuggedSwitch family meets and exceeds recognized industry standards (e.g. IEC 61850-3, IEEE 1613, NEMA TS 2) for ruggedness and communications performance and is well suited for mission critical real-time control applications requiring high levels of reliability and availability.

Figure 24. RuggedSwitches from RuggedCom.

RuggedMAX is a high-performance, long range, secure family of products, fully compliant with the WiMAX 802.16e Wave 2 (MIMO) mobile broadband wireless standard. RuggedMAX is designed to extend IP networks over large distances to fixed and mobile users. The product family includes a variety of base stations and subscriber stations with differing output powers, form factors and frequency options for use in licensed or license exempt bands. The RuggedMAX product family has gone through extensive end to end network interoperability testing to support multiple different ASN gateway platforms and 3rd party subscriber devices in order to give customers flexibility by leveraging the full WIMAX ecosystem. RuggedMAX Wireless Broadband WiMAX Technology, with its compact form factor and flexible configuration, suits mission critical private networks well.

Figure 25. RuggedWireless products from RuggedCom.

Last but not least, the RuggedGRID solution provides communications that is Utility Grade meaning it has characteristics and performance levels as required for the Substation Environment, as explained in www.ruggedcom.com/applications/electric-utilities/. RuggedCom has one of the industry's most complete basket of networking devices designed specifically for the substation environment. This range of products is available in the context of an IEC 61850 substation. However, other network architectures such as ring or star topologies, or a hybrid topology, are also accommodated.

9 Conclusions

Smart Grid is about interconnected IT systems controlling the “dumb” power systems, thus communication plays crucial part in the picture. As the Smart Grid covers everything from centralized generation to the end consumers and homes, also the communication requirements have multiple and sometimes conflicting aspects.

Traditionally electric utilities have been deploying application and system specific communication solutions, owned and operated by themselves. However, the learning from other industries, especially from telecommunication and Internet, show that only common, shared, standardized communication infrastructure provides the basis for successful innovation of new services and business.

Smart metering and wide spreading of distribution automation bring fundamental change to the communication requirements from two aspects. Firstly the number of endpoints will increase 100-1000 times or more and secondly the cost of communication will play significant role (especially in smart metering).

As the electric grid is counted as critical infrastructure the availability and security requirements play central role. However, there are different views how to achieve the goal. As an example some think that closed proprietary systems are more secure than open and standardized. This view has been proven to be wrong long time ago in the IT world.

The operational requirements vary greatly depending on the application. Some applications, like teleprotection, may have such strict delay and/or availability requirements that it may not be economically feasible to integrate those into the generic communication infrastructure. The smart grid devices are located in many cases in harsh environments. This brings the requirement of extended environmental durability (temperature, humidity, vibration).

The evolution of the grid may speed up along the time, but still it is evident that the lifecycle of the technology will be longer that in common ICT. This brings the need of easy upgradeability and future proof solutions.

The electric industry is facing major business environment disruption caused by the market liberalization and other regulatory changes. This will bring new (types of) players into the game. From this angel the smart grid communication networks need to be built to support services and applications, which have not yet been invented.

The last observation to be mentioned could be the fact that there are fundamental regional differences (grid architecture, political, regulatory, building culture, existing ICT networks, geography, climate, and so on).

10 Acknowledgements

This document has been created by the TEKES funded SGEM project WP4.1.4: “Tools and methods for telecommunication”. The editors thank all SGEM partners for valuable information and feedback which made this compilation possible. Special thanks to Jani Valtari (ABB) who provided his deep insight in distribution automation.

11 References

Source /1/:“European Smart Grids Technology Platform- Vision and Strategyfor Europe’s ElectricityNetworks of the Future”, EU Comission/Community Research, 2006

Source /2/: “What you should know about the electricity market”, Finnish Energy Industries and Fingrid Oyj).

Source /3/: Wiki *http://en.wikipedia.org/wiki/Distributed_generation*

Source /4/: Electricity retail markets in Europe – division of duties between suppliers and DSOs, Thesis work at Lappeenranta University of technology, 2008

Source /5/: Ideas taken from preliminary document: THE FINNISH ELECTRICITY RETAIL MARKET, 22.2.2010 by Anna Sahari

Source /6/: http://www.verisae.com/page/1/energy-aggregators.jsp and *http://seekingalpha.com/article/191614-aggregation-will-destroy-niche-markets-for-smart-grid-energy-storage*

Source /7/: http://www.meteroperators.org.uk/

Source /8/: Lilakiatsakun, W., Seneviratne A. Wireless Home Networks Based on a Hierarchical Bluetooth Scatternet Architecture.

Source /9/: M2M, Mission Critical Thoughts V0.06, 2010-8-18, Owner: Sampo Yliraasakka http://www.cleen.fi/research/images/0/0f/M2M_Mission_Critical_006_18082010.pdf

12 Appendix A: List of Abbreviations

3G	Third Generation of standards for mobile communications and services
3GPP	Third Generation Partnership Project
4G	Fourth Generation of standards for mobile communications and services
AC	Alternating current
ACSI	Abstract Communication Service Interface
ADA	Advanced Distribution Automation
ADSL	Asymmetric Digital Subscriber Line

AES	Advanced Encryption Standard
AIPN	All IP Networks
AMI	Advanced Metering Infrastructure
AMIS	Automated consumption data acquisition and information system
AMR	Automated Meter Reading
ANSI	American National Standards Institute
AP	Access Point
API	Application Program Interface
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
ASDU	Application Service Data Unit
ASHRAE	American Society of Heating, Refrigerating and Air Conditioning Engineers
ASN.1	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
ATU	ADSL Terminal Unit
BAS	Building Automation System
BPEL	Business Process Execution Language
BPL	Broadband over Powerline (see also PLC)
BPMN	Business Process Modeling Notation
CAPEX	Capital expenditure
CATV	Cable TV
CDM	Code Division Multiplexing
CDMA	Code Division Multiple Access
CdTe	Cadmium telluride
CEA	Consumer Electronics Association

CERT	Computer emergency response team
CGR	Connected Grid Router
CGS	Connected Grid Switch
CHP	Combined heat and power
CIGRE	International Council On Large Electric Systems
CIM	Common Information Model for energy management applications
CIP	Critical Infrastructure Protection
CIS	Component Interface Specification
CM	Configuration Management
COTS	Commercial off-the-shelf
CPP	Critical Peak Pricing
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
Cu	Copper
DA	Distribution Automation
DC	Direct current
DEMS	Decentralized energy management system
DER	Distributed Energy Resources (distributed generation and storage)
DES	Data Encryption Standard
DG	Distributed generation
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security (USA)
DIN	German Institute for Standardization
DisCo	Distribution company

DIY	Do It Yourself
DKE	Deutsche Kommission Elektrotechnik
DMS	Distribution management system
DMT	Discrete-Multi-Tone
DMZ	Demilitarized zone
DNP/3	Distributed network protocol
DNS	Domain Name System
DOD	Department of Defense (USA)
DOE	Department of Energy (USA)
DP	Dynamic Pricing
DR	Demand Response
DS	Distribution System
DSL	Digital subscriber line
DSLAM	Digital Subscriber Line Access Multiplexer
DSO	Distribution System Operators
EAI	Enterprise Application Integration
EAN/EDIEL	Business process model for invoicing in downstream electricity power market
ebIX	European forum for energy Business Information eXchange
ebXML	Electronic Business (eBusiness) eXtensible Markup Language
EDGE	Enhanced Data rates for GSM Evolutions
EDI	Electronic Data Interchange
EDL	Exchange Data Language
EDP	Electronic data processing
EHV	Extra high voltage

EIA	Electronic Industries Alliance
EIB	European Installation Bus
EISA	Energy Independence and Security Act
ELCOM	Electricity utilities communication
EMC	Electromagnetic compatibility
EMI	ElectroMagnetic Interference
EMS	Energy Management System
EN	European Standard
EPRI	Electric Power Research Institute
ES	Energy Storage
ESP	Energy Service Provider
ETC	ebIX Technical Committee
ETSI	European Telecommunications Standards Institute
ETSO	European Transmission System Operators
EU	European Union
EV	Electric Vehicle
EWG	Electricity Working Group
FACTS	Flexible AC transmission system
FCC	Federal Communications Commission
FDD	Frequency Division Multiplexing
FEC	Forward Error Correction
FERC	Federal Energy Regulatory Commission
FO	Fiber optic
FTP	File Transfer Protocol
GenCo	Generation company

GHG	Greenhouse Gases
GID	Generic interface definition
GIS	Geographic Information System
GOOSE	Generic Object Oriented Substation Events
GPRS	General packet radio service
GPS	Global Positioning System (time source)
GRS	General Radio Service
GSM	Global system for mobile communications
GTIN	Global Trade Item Number
GUI	Graphical user interface
GWAC	GridWise Architecture Council
HCC	Home Control Center
HDSL	High Data Rate Digital Subscriber Line
HDTV	High Definition TV
HF	High frequency
HMI	Human Machine Interface
HSDPA	High-Speed Downlink Packet Access
HSxPA	High Speed Xlink Packet Access
HTTP/HTTPS	Hypertext transfer protocol/ hypertext transfer protocol secure
HV	High voltage
HVAC	Heating Ventilating and Air Conditioning
HVDC	High voltage direct current
HVDCT	High voltage direct current transmission
HW	Hardware
ICCP	Inter-control center communication protocol

ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IED	intelligent electronic device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHD	In-Home Display
IMT	International Mobile Telecommunications
IO	Input Output
IOS	Internetwork Operating System
IP	Internet Protocol
IS	International Standard
ISDN	Integrated services digital network
ISM	Industrial, Scientific and Medical band
ISO	International Organization for Standardization, Independent Systems Operator
IT	Information Technology
ITU	International Telecommunication Union
KNX	Network communications protocol for intelligent buildings
LAN	Local Area Network
LCD	Liquid crystal display
LED	Light emitting diode
LTE	Long Term Evolutions
LV	Low voltage
LVMD	Low voltage main distribution

M2M	Machine to Machine
MAC	Message Authentication Code
MD	Main distribution
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MIMO	Multiple Input Multiple Output
MMS	Manufacturing Messaging Specification ISO 9506
MSCONS	Metered Services Consumption
MTBF	Meantime between failures
MTTF	Meantime to Failure
MUX	Multiplexer
MV	Medium voltage
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Council / Corporation
NFC	Near Field Communication
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NTP	Network time protocol
NTT	Nippon Telegraph and Telephone
OASIS	Open Access Same Time Information System
OASIS	Organization for the Advancement of Structured Information Standards
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier

OMG	Object management Group
OpenSG	Open Smart Grid
OPEX	Operational expenditure
OSGi	Open Services Gateway Initiative
OSI	Open Systems Interconnection (Basic Reference Model)
PABX	Private Automatic Branch Exchange
PCM	Pulse code modulation
PDH	Plesiochronous digital hierarchy; an international multiplexing standard
PDU	Protocol Data Unit
PEV	Plug-in Electric Vehicles
PLC	Power-line carrier
PMU	Phasor Measurement Unit
POTS	Plain Old Telephone Service
PPPoE	Point-to-Point Protocol over Ethernet
PROFIBUS	Process Fieldbus
PSTN	Public Switched Telephone Network
PUC	Public Utility Commission
PV	Photo-Voltaics
QOS	Quality Of Service
RAN	Radio Access Network
RES	Renewable energy sources
RF	Radio Frequency
RFC	Request for Comments; Remote Feedback Controller
RFID	Radio Frequency Identification
RJ	Registered Jack

RMS/ rms	Root mean square
RSA	Rivest, Shamir, Adelman
RSTP	Rapid spanning tree protocol
RTO	Regional Transmission Operator
RTP	Real-Time Pricing
RTU	Remote Terminal Unit
SAE	System Architecture Evolution
SAS	Station automation system
SCADA	Supervisory Control And Data Acquisition
SCL	Substation Configuration description
SDH	Synchronous digital hierarchy; multiplexing protocol for transferring multiple bit streams over the same optical fiber
SDO	Standards Development Organization
SDSL	Synchronous Digital Subscriber Loop
SFPs	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SHA-1	Secure-Hash-Algorithm Version 1
SHDSL	Symmetrical High Data Rate Digital Subscriber Line
SIMs	Subscriber Identity Module
SLA	Service Level Agreement
SMTP	Simple Mail transfer Protocol
SNCP	Sub-network connection protection
SNMP	Simple network management protocol
SNTP	Simple Network Time Protocol
SOA	Service-Oriented Architecture

SONET	Synchronous optical network
SQL	Structured Query Language
SSH	Secure Shell
STATCOM	Static synchronous compensator
STM	Synchronous transport module
SVC	Static var compensator
TCP/IP	Transmission Control Protocol/Internet
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TETRA	TErrestrial Trunked RAdio (ealier: Trans European Trunked RAdio)
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework
TOU	Time-of-Use
TransCo	Transmission company
TSO	Transmission System Operator
UHF	Ultra high frequency
UHVDC	Ultra-high-voltage direct-current
UI	User Interface
UID	Universal Identifier
UMB	Ultra Mobile Broadband
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
UPnP	Universal Plug and Play
UPS	Uninterruptible power supply

USB	Universal serial bus; serial bus standard to interface devices
UTRAN	UMTS Terrestrial Radio Access Network
VDSL	Very high bit-rate Digital Subscriber Line
VHF	Very high frequency
VID	VLAN Identificator
VLAN	Virtual LAN
VLF	Very Low Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPP	Virtual power plant
VT	Voltage transformer
W3C	World Wide Web Consortium
WAMS	Wide-Area Measurement System
WAN	Wide area network
WAP	Wireless Application Protocol
WASA	Wide Area Situational Awareness
WCDMA	Wideband Code Division Multiple Access
WDM	Wavelength division multiplex
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMAX	Worldwide interoperability for microwave access
WLAN	Wireless local area network
WP	Work Package
WPAN	Wireless Personal Area Network

WS	Web Services
WSDL	Web Services Description Language
XML	Extensible markup language