DREAM Phase 1 – Appendix to main report

Appendix 8

A Survey of Smart Grid Communication with focus on Embedded Systems (in English)

ForskEL projekt nr. 10744

Project partners:

A Survey of Smart Grid Communication with focus on Embedded Systems

By Theis Solberg Hjorth, Danfoss Power Electronics

2014-01-31

A contribution to phase 1 of the ForskEL Project DREAM - “Danish Renewable Energy Aligned Markets”

A Survey of Smart Grid Communication with focus on Embedded Systems

Contents

Introduction

According to the EU Joint Research Centre (JRC), the definitions of Smart Grid are[3]:

EU definition: "A Smart Grid is an electricity network that can intelligently integrate the behaviour and actions of all users connected to it- generators, consumers and those that do both- in order to efficiently ensure sustainable, economic and secure electricity supply" [EC Task Force for Smart Grids, 2010a]

US definition: "A Smart Grid uses digital technology to improve reliability, security, and efficiency (both economic and energy) of the electric system from large generation, through the delivery systems to electricity consumers and a growing number of distributed-generation and storage resources "[US DOE, 2009a]

Commercial power electronics products will play a role in various Smart Grid settings sometime in the future and they will need to connect to and communicate with controllers and other components in the systems, they reside in. There is no unique standard for this communication yet besides the IEC 61850 originally intended to facilitate grid control at the substation level and above. Two main challenges, we face are hence 1) the uncertainty of how Smart Grid communication standards will evolve and 2) the lack of suitable standards for Smart Grid communication for embedded systems (IEC61850 carries some overhead and requires processing capacity beyond small embedded systems).

The purpose of this document is to survey existing communication technologies and methods within Smart Grid and Smart Energy. For emerging methods, pros and cons are listed.

The term Smart Energy is increasingly being used instead of Smart Grid since the research subjects and industrial focus is moving towards energy storage, renewable energy sources, and energy optimization methods, in contrast to simply moving energy around. Despite this, funding is still granted for these types of projects under the name of Smart Grid.

General Smart Grid Progress

The current state of investments and ongoing projects related to Smart Grid are monitored in the EU by the Joint Research Centre (http://ses.jrc.ec.europa.eu) and in the USA by the Virginia Tech Smart Grid Clearinghouse (http://www.sgiclearinghouse.org/AboutSGIC)

Smart Grid dissemination platform shows projects and a map of them in the EU: https://portal.smartgridsprojects.eu/Pages/Map.aspx

In China[5], the State Grid Corporation of China (SGCC) is the driving force behind their efforts to build a nationwide Smart Grid. They have recently made a deal with the USA for joint effort on this. The distribution grid is less mature than developed countries, so China is investing mainly in smart meters, more efficient distribution transformers, and a large capacity interconnected transmission backbone.

The power grid of India[5] suffers from a staggering 50% average transmission and distribution loss. They are investing in transmission efficiency technology as well as renewable energy sources.

South Korea, Australia, Japan and Brazil are investing moderately[5]. They either roll out smart meters, use more renewable energy sources, or are looking into small scale Smart Grid demonstrations projects.

In the EU, Denmark, Germany, Spain and the UK together account for half of the total number of Smart Grid projects[5]. Denmark alone participates in 22% of Smart Grid projects.

Denmark stands out in terms of the number of R&D and demonstration projects[5]. This is partly explained by the fact that Denmark has already achieved a very high penetration of renewables and distributed generation. Moreover, the Danish TSO (Transmission System Operator) is charged with supporting R&D and demonstration activities in the electricity sector, activities which are then financed through a Public Service Obligation (PSO) tariff. Under the PSO program ForskEL, the Danish TSO administers funding of 130 million DKK a year. This system also implies the traceability of the projects which can then be easily monitored and communicated, favoring the assessment of their results and knowledge sharing.

EU Smart Grid State-of-the-Art 2012

This section is a summary of the EU Smart Grid projects 2012 report[6]:

Projects focusing on distributed ICT (Information and Communication Technology) architectures for coordinating distributed resources and providing demand and supply flexibility are probably in the majority:

- distributed intelligence/multi-agent architectures are widely adopted at technical level, with successful trials of technical VPPs (Virtual Power Plants), e.g. coordination of DERs (Distributed Energy Resource) for voltage regulation
- a lack of standardized control and communication solutions means that costly ad-hoc configuration is required, which limits the participation of (in particular, small-scale) users;
- more trials are needed to test the scalability of developed platforms, especially when real-time grid requirements and market signals have to be taken into account;
- at market level, the main focus is on analyzing the market potential of aggregation schemes and the viability of business models;

Recently, a few large scale demonstrators have been launched to test VPP coordination with market signals and grid constraints (integrated technical and commercial VPP). Scalability is a major focus, especially when thousands of agents need to be coordinated. Trials still involve limited numbers of users and consumer resistance to participation in trials is still high;

Focus on storage appears to be on the rise. Use of storage as additional source of grid flexibility is one of the key themes of the main projects that started in 2012.

On the basis of official commitments or strong interest from several Member States in the smart metering roll-out, it is estimated that at least € 30 billion will be spent and at least 170-180 million smart meters will be installed in EU-27 by 2020;

- Investment cost per smart metering point varies widely, from less than € 100 to € 400, depending on scale, what functionalities are implemented, communication technology and specific local conditions;
- The most common key monetary benefits of smart metering are energy savings, reduced meter readings and operational savings for the utility, e.g. technical and non-technical losses. Additional benefits are expected from the applications the smart meters will enable (e.g. demand response, new innovative services for consumers, etc.);
- The choice of a particular communication option is strongly dependent on the local conditions. However, available information indicates that the most widespread communication option is the combined use of PLC (power line communication) for the Smart Meter-Concentrator connection in the secondary substation and the use of GSM/GPRS for the Concentrator-Meter data management system connection;
- Multi-utility configuration (installation of water and gas meters together with electricity smart meters) is tested in a small minority of the projects surveyed. There still seems to be uncertainty as to

whether the additional benefits of multi-utility configuration compensate the costs.

Denmark and Germany are the leading countries with projects focusing on consumer engagement.

Obstacles

Regulatory and market barriers seem to be the main obstacles to the development of commercially viable aggregation applications, e.g. establishing clear rules for the technical validation of flexible supply/demand (demand-response) transactions by system operators; technical/commercial arrangements for the exchange of physical and market data; clear market roles and responsibilities and fair sharing of costs and benefits; new contractual arrangements;

Key barriers appear to be policy-related, social or regulatory, rather than technical:

- Lack of interoperability and standards (standardized plug and play would reduce costs and allow connectivity also of small DERs or small DR applications);
- Regulatory barriers: uncertainty over roles and responsibilities in new smart grid applications; uncertainty over sharing of costs and benefits and consequently over new business models;
- Consumer resistance to participating in trials;
- The range of regulatory arrangements in Europe might present significant barriers to the replicability of project results in different countries.
- Data collection and dissemination
- To support the transition to a smart grid, it is crucial that project information is shared. However, there are many barriers to this: web information about projects is difficult to retrieve; many projects do not have a dedicated website; in some cases, websites are only in the national language;
- Making European funding subject to the extensive sharing of project results greatly contributes to knowledge-sharing in the smart grid community. Typically, EU-financed projects provide the most detailed and accessible information;

The most common technical obstacle reported was the lack of interoperability between different smart grid elements, e.g. the incompatibility of the different IT protocols and components (BeMobility 2.0), the lack of communication standards for EVs (Context Aware Electric Vehicle Charging Based on Real Time Energy Prices), the completely different communication standards of smart grid devices (PREMIO) or the lack of standards in the interoperation of home gateways with smart grid applications (Encourage).

Standardization Efforts

From [3]: "In March 2009, the Commission issued mandates to the European Standardization Organizations (ESOs), namely CEN, CENELEC and ETSI, for standardization of smart meters. In June 2010 ESOs initiated development of standards for charging electric vehicles. Recently, the Commission launched a mandate for Smart Grids aimed at developing standards facilitating the implementation of different high-level Smart Grid services and functionalities defined by the Task Force [EC Task Force for Smart Grids 2010a, 2010b, 2010c]. The identification of standard gaps is performed through a Smart Grid reference architecture, which identifies the different subsystems composing the Smart Grid and represents the functional information data flows among them. A report on "Standards for Smart Grids" [CEN-CENELEC-ETSI, 2011] has been issued in May 2011. The European Commission has also created a Smart Grids Reference Group (now working within the framework of the Smart Grid Task Force) to monitor implementation of the work program established with a view to ensure timely adoption of the standards [EC 2011a]. Besides the technical specifications, the mandate for Smart Grids also contains elements related to data protection and data privacy, which is a key issue for the deployment and acceptance of Smart Grids [EC Task Force Expert Group 2010b; EC 2012c]"

In the USA[3], NIST created the Smart Grid Interoperability Panel (SGIP) to help coordinate development of Smart Grid standards. SGIP is a consensus-based group of more than 675 public and private organizations, and they publish the IKBFramework (Roadmap for interoperability). In July, 2011, the Smart Grid Interoperability Panel published the first six entries of its new Catalogue of Standards[4], a technical document now available as a guide for all involved with Smart Grid-related technology. BACnet and IEC 61850 are part of the portfolio of standards mentioned here.

Some core IEC standards worth mentioning are: 61850 (substation automation), 61970 (Common Information Model), 61968 (app integration at electric utilities), 62351 (security for 61850 and others).

Smart Grid in the EU vs. USA

There are some key differences between the Smart Grid efforts in the EU and those in the USA. The basis of the Smart Grid concept can in some senses be traced to the IEC 61850 standard on the design of Electrical Substation Automation. Previously many different proprietary standards existed for exchanging data between different vendors in substations. This led to difficulties in the USA resulting in either unpowered substations (because no supplier was leading power to it), or explosive failures (when too many suppliers were leading power to it).

The EU power distribution grid has historically been more interconnected than the USA one and the ability to share and move power between countries when needed has resulted in a very stable supply, both in terms of uptime/reliability and in terms of guaranteed supply (supply security). In the USA, particularly in California and the North-East, there have been major blackouts and brownouts during peak hours and low supply security and reliability[19]. Hence the USA has been working on Smart Grid efforts for longer than the

EU, and for different reasons. The USA Smart Grid is focused on a Demand-Response model in which power suppliers and consumers create legal contracts that allow the supplier to order the consumer to lower their consumption on demand. For instance, a contract will allow the supplier to send a signal commanding the consumer to reduce their power consumption by 30% for the next 2 hours. The remuneration, maximum length of time, and maximum percentage of reduction are all specified in the contract. This system requires separate legal contracts, which are usually only made with large companies, due to the legal overhead and the cost of the specialized equipment needed to send, receive, and react upon these signals. Nevertheless, the system helps flatten peak power consumption in a dynamic way.

In the EU, this issue generally is not found and certainly not to the extent of the supply problems in the USA. When suppliers are short, they buy power from another country and when they produce too much, they sell it again. Looking ahead, however, the switch to renewable energy sources that can be unpredictable, the need to optimize power usage, and the growing energy consumption will necessitate the creation of a Smart Grid. More specifically[5], "Due to a more marked time-variability and weather-dependence of its energy output (compared to other generation technologies), the balancing task of power system operators becomes harder to carry out; as a matter of fact, since electricity is not stored on a massive scale to date, the power produced must at all times equal the power consumed (and lost)."

But at the moment the EU is not in a power supply reliability crisis situation as the USA is (in some states), so the urgency of adoption is very different. This is also reflected in the research and industrial projects that are invested in. The projects in the USA seem more focused on existing or near-future issues, whereas projects in the EU focus more on long-term perspectives. Policy-making at the EU level also shows a lack of direction, e.g. laws on subsidizing of solar panels are changing every few years in different countries, creating a turbulent market situation. In the USA, the SunSpec Alliance[7] created a draft addendum to the safety and communication standards governing solar devices (Meters, Inverters, etc.) in the beginning of 2013; by early 2014 this standard will be mandatory according to California law. This example shows the heavy involvement and focus of governmental bodies in the development of solar standardization efforts.

Smart Grid Communication

The focus of this report is on the possibilities in Smart Grid communication. The previous sections should have made it clear that a standardization effort in this area is still a long-term prospect, so we will look at a variety of methods and suggestions that have been used in projects, and look at the pros and cons of each.

Introduction to Communication

The report “Smart Grid projects in Europe”[5] from the JRC maintains a category number four named “Integrated System” which focuses on the integration of different Smart Grid technologies and applications, e.g. Smart meter, Demand Response, grid automation, distributed storage, renewables, etc. Projects in this category are most likely to be dealing with communication and interoperability issues.

Demand Response (DR)[5] is a central theme in Smart Grid projects. It is “the active participation of commercial/domestic consumers in the market through the provision of consumption flexibility services to different players in the power system. This is achieved by aggregating consumers’ reduced load into larger amounts for participation in market sales (e.g. to sell to network companies, balancing responsible parties, owners of non-controllable generation, etc.). Aggregators are the key players to mediate between consumers and the market. Particularly challenging is the integration of domestic consumers who, as opposed to DG (distributed generation) and large industrial consumers, are less motivated by purely economic concerns (minimal gains). Furthermore domestic consumers are generally unable to make precise predictions on their available load flexibilities; therefore it is difficult for them to ‘offer’ services in the classical sense. Rather, the idea is for their services to be made available at the market’s ‘request’, i.e. through price and/or volume signal mechanisms, and for the provision of services to be on a voluntary and contractual basis.”

“Demand Response projects testing dynamic pricing and consumer participation, are growing in number. They are benefiting from the deployment of **smart meters, which are key enablers** for the increase of Demand Response initiatives. More and more Demand Response projects are moving from R&D applications to demonstrations to test actual consumer engagement. Gaining consumers trust and participation is the main challenge in this field. Potentially, consumers’ benefits are significant. They range from energy savings (up to 10-15%) to a more favourable business case for the purchase of home energy resources (heat pumps, EVs, CHPs etc.) through a direct participation in the electricity market (selling power and/or load flexibility). However, in order to capture most of these benefits the whole system (infrastructure + market) needs to be in place.”

Generally the Smart Grid communication can be said to consist of two layers: the Physical Layer (the infrastructure for power and data flows between producers and consumers), and the Market Layer (mechanisms for coordinating transactions between operators, prosumers, aggregators, etc.). In addition, energy management devices are envisioned to separate a consumer’s system from the outside world. It can be a hub for smart home energy services or building management systems, and it will reshape the energy profile of the building according to outside inputs such as current market value of energy, current energy need, etc. It will be the recipient of Demand Response signals from the Smart Grid and will react accordingly, either turning on or off the consumer's electrical loads according to pricing and personal requirements. Since the energy consumption of homes and end-users are small compared to the total consumption, aggregators will act as intermediaries, collecting and collating many consumer energy profiles into large virtual power units to sell or buy in bulk from producers.

See the Appendix for a list of EU Smart Grid projects that have worked with communication. The results of these projects should be investigated further to establish a full picture of related work.

Communication Security

This section summarizes information from the EU Smart Grid 2010 report[5]:

Given the interdependence of existing energy and information infrastructures, the electricity sector also feels the impact of mounting cyber security concerns. Along with big opportunities of Smart Grids comes the bad news that the next generation of Europe's electricity grids will face a greater variety of cyber vulnerabilities than those of today. Therefore a special emphasis is put on critical infrastructure protection, especially infrastructure supporting energy, transport, telecommunications, and water.

From the data protection and security point of view, five important challenges arise:

1) the large amount of sensitive customer information the grid will transmit;

2) the greater number of control devices in the Smart Grid;

3) the poor physical security of a great proportion of these devices;

4) the use of Internet Protocol (IP) as a communication standard;

5) the greater number of stakeholders the grid will rely on for its smooth operation.

The responses received from project coordinators have been generally quite poor in data protection and security. Therefore, the analysis in this section is mostly based on the results of the OpenMeter project, by far the most significant and detailed project.

- A scan of collected projects highlights the convergence towards IP communication and other standards-based solutions. The promises of Smart Grids will only realize if low-priced consumer devices are available.
- Proven standards and industry best practices used for IT systems should be considered and adapted, and security measures not reinvented. Open standards at the European and international level are necessary for updating and upgrading the security mechanisms of these devices as threats and risks evolve.
- Most of collected projects have not provided responses on data protection and security. It seems that the potential to tackle this issue is not fully exploited. New projects focusing on data handling would be useful to assess how data handling principles from other industries (e.g. banking industry) can be

applied to Smart Grids.

- Smart Grid projects require the collaboration of several players with different competencies and background. Since security in the ICT infrastructure is a collective effort, it is imperative that roles and responsibilities are clearly defined and that both the energy and ICT communities work together to coordinate security measures to prevent blind spots.
- An open and secure ICT infrastructure is at the core of a successful Smart Grid implementation. Addressing interoperability, data privacy and cyber-security is a priority requirement to make the ICT infrastructure truly open and secure.
- A privacy-by-design approach needs to be adopted to ensure customer security. A wide consensus among stakeholders is emerging in Europe on this.

It seems clear that a paradigm shift is needed in energy industry from the current hardware-centric focus on system adequacy and reliability, towards the inclusion of a more directly consumer-oriented view of security.

Privacy by design aims at building privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles http://www.edps.europa.eu/EDPSWEB/edps/EDPS

At the European level, there is a general agreement among stakeholders that Smart Grid solutions have to comply fully with the binding rules on privacy and data protection. A privacy-by-design approach needs to be adopted to ensure customer security. This approach has been integrated in the Mandate M49012 for European Smart Grid standards, issued early in 2011. Furthermore, the European Commission is also ready to support the Member States in ensuring, when deciding of roles and responsibilities regarding ownership, possession and access to data.

Communication Security - Analysis and Discussion

As the report cited in the section above states, despite many Smart Grid initiatives mentioning cybersecurity as an important pillar of the system, not many research projects or company products focus on this aspect. Looking at existing low-level communication technologies (e.g. IP, ZigBee, 6lowpan, Ethernet, Modbus, UMTS, M-bus, etc.), just about every technology has implemented a different kind of security, while some technologies have no security. This necessarily means security must be implemented at the application layer (if XML, e.g. by using the WS-Enc standards). This provides a way to secure communications, even though the transport technologies are still years away from implementing a proper, peer-reviewed security technology. In light of recent NSA revelations[20], we do not know what to trust anyway, and flexibility becomes paramount, especially considering that security built into communication stacks and/or hardware takes a lot of effort to update if vulnerabilities are found. This flexibility is maximized, if the application layer intrinsically supports security, and does away with the huge problem of guaranteeing certain security properties of data transfers when these pass through an unknown number of unknown transport layers with different levels of security.

Sometime in the (distant) future when we are certain that all the communication technologies being used have proper security measures, the application layer security may be relaxed or delegated to lower layers.

In the current state of affairs, the worst thing to do when designing future Smart Grid communication systems, would be to let the communication technology at the lower layer handle security. Since the Smart Grid application layer inevitably must be agnostic about the transport layer (if for no other reason than the fact that there are many different incompatible systems already deployed), there cannot be any guarantees at the application layer that the messages being sent will be secure, simply because the lower layers could be different for every system and have their own methods and levels of security. Therefore the short-term to mid-term solution must be a focus on “message-level” or “message-oriented” security at the higher layers, e.g. the application layer.

A comprehensive security risk analysis of the Smart Grid is also lacking. The vision of the EU Smart Grid is basically to create a massive M2M (Machine-to-Machine) stock market for all intelligent electrical appliances. The amount of money and therefore potential fraud involved in this system will be substantial.

In the case where every country/power company will choose their own cloud provider for the ‘smart’ part of the Smart Grid, a number of unanswered questions arise:

- What is the risk for market and technology fragmentation?
- Will cloud services be able to access each other?
- What is the data exchange format for bidding on, controlling, and paying for resources?
- What ensures openness and interoperability in the system?
- What prevents fraud?
- How is cloud migration without prohibitive costs ensured? Consider platform lock-in, data lock-in, tool lock-in, vendor lock-in, supplier lock-in.
- What happens when the cloud is unavailable? (even Amazon EC2 only has 99.95% uptime). Is the cloud critical? Will millions be lost in wasted energy and money if the cloud is unavailable? Will homes and buildings lose power?
- What is the risk assessment of unavailability of DER resources? (There are a few projects looking into this, the term they use is ‘island systems’ for sudden isolations of part of the grid).
- How are the data ownership concerns inherent in cloud computing handled? Both ownership of private consumer data and ownership of the aggregated data if the cloud provider is not in the EU. Privacy and anonymity issues also arise when traffic analysis can be used to check when people are at home, and - by looking at the consumption signatures of devices - what they are doing.

Technical Communication Issues

The models used to describe the data flows and interactions between systems in the Smart Grid are very complex. These are usually in UML format, or XML when parts of them need to be machine-readable. An issue that seems often overlooked in Smart Grid communication projects is the aspect of the resource limitation of the small embedded systems that are actually supposed to parse this information. Particularly in research projects involving universities, the focus is on fast prototyping and proof-of-concepts, which means that the implementations are often made with Java or Python and either simulated on a laptop, or using microprocessors that far exceed the processing power of an actual commercial product. This is fine to test theories, but the issues arise when the protocol designs are also made in this way, without keeping in mind what the actual commercial processing environment is likely going to be, i.e. not considering compression or brevity of data signals into a protocol design, because the proof-of-concept that is being built is running on a PC that has no such bandwidth or memory limitations.

For example, designing an XML format that creates messages which take up 1MB of data for transferring a weather forecast are simply infeasible for the microprocessor on a heat pump device to contain, or even transfer within a reasonable amount of time. The commercial reality is that every component must be made to specification, and e.g. having to switch to a microprocessor that costs €2 more in each product can amass to millions in lost profit annually for the company. Contrary to popular belief, the effect of Moore's Law is only applicable to products with such a high economy of scale that the annual turnover is measured in multi-digit $billions, because this enables billions to be spent on research. It is quite a different story for the chips used in embedded systems that are not as standardized or have such a high economy of scale.

Some general technical issues:

- Small embedded systems are resource-constrained in terms of memory, storage, processing power, battery power.
- There are NAT issues when using Internet Protocol.
- IPv6 is more complex than IPv4, but necessary for the Internet of Things.
- There is no communication standard for Smart Grid.
    - Anything from wind mills to temperature sensors are part of the Smart Grid, so it is unlikely that one communication standard will ever emerge, since the types of devices that should be a part of a Smart Grid vary wildly in terms of resources: Processing power, memory, battery life, wireless/wired protocols.
    - There is no 'one-size-fits-all' communication protocol, especially for wireless low-power devices. Hence Smart Grid will always be a heterogeneous network. This means there will be gateways to translate the physical network technologies, but there need not be application layer gateways if the application layer protocol is designed to accommodate all the different devices that will be part of the Smart Grid.
    - The lack of standards means that vendors wanting to get early to the market will invent their own ad-hoc, incompatible, proprietary protocols. An open protocol standard is unlikely to emerge from vendors; there must either be a political demand, the outcome of a research

project, or an alliance of vendors in order to create such a standard.
    - IP, or protocols on top of IP are popular candidates, however, IP was not designed with embedded systems in mind.
        - The advantage of IP is the ubiquity and openness, and that it is used in many higher layer data transfer frameworks, which makes it simple to use for fast prototyping. The disadvantages are that it is not a light-weight protocol and it makes assumptions about online availability. IP assumes that devices are always available on the network, which is not the case for low-power devices that spend most of their time asleep to save power.
- The centralized retail/industry mindset of, for instance, OpenADR in which a server is deployed to control a building, does not fit well with consumer-level requirements. Such a server requires expert knowledge to commission and maintain. This knowledge is not available to the ordinary consumer, and experience shows that software setup, update, and maintenance cannot be reliably delegated to consumers either.

Control Intelligence

Somewhere in the Smart Grid there must be some control intelligence that can interpret the signals coming from the grid and decide what to do. The signals can be commands to save energy, or information about current energy prices. We may distinguish between two types of signals:

- Commandable: direct control (e.g. 'reduce power by 20% for the next 2 hours'). Requires knowledge about the device being controlled and how to control it. Requires action or response from the device. There is a static binding between controller and device.
- Informational: indirect control (e.g. weather forecast, energy price forecast). Does not require knowledge of the device, does not enforce any action. No static binding between devices.

A reaction to a signal may be to turn on/off, or adjust usage of certain connected devices according to a schedule, a desired energy profile, etc. An Energy Management Device (EMD) can be used in commercial and retail systems that ordinarily have some server in a Building Management System (BMS) that contains this control intelligence. These systems are expensive, need maintenance, and require expert knowledge to configure. The systems are usually proprietary and use dedicated signal lines to connect to the equipment distributed in the building, such as temperature and CO_2 sensors, and HVAC systems.

Residential EMDs will need to be far more user-friendly and open to drive prices down. The same kind of gatekeeper vendor that owns the system is infeasible in this market, simply due to the way it would stifle innovation, make the system too expensive, and would require that the gatekeeper creates or is involved in the creation of every residential smart device (coffee machines, lighting, fridges, HVAC, anything that would benefit from being connected to the Smart Grid/Internet). Considering the amount of different types of devices that could conceivably be energy managed and the different communication protocols and physical mediums that they would use, makes this market too great for any one gatekeeper vendor to control.

The location of control intelligence is also an interesting problem in the residential environment. Clearly standardization of command/information signals is needed within the heterogeneous network, which means that control intelligence becomes more decentralized. As mentioned previously, in the commercial setting the control intelligence resides on one, high-maintenance BMS server. This is possible because the system is relatively closed and can only be used with a limited number of devices (e.g. Modbus sensors or BACnet HVAC systems); in other words, the system is commissioned and tested, and is then statically configured. However, a residential setting must be dynamic (since the user can buy a new gadget and connect it at any time), and an EMD built on the same principles as the BMS server cannot offer this. Essentially the EMD does not know what will be connected to it and what it will be controlling, hence the control intelligence must be delegated (to some degree) to the connected devices.

There are three scenarios of interest: either the EMD has full knowledge of the devices connected and can control them all (centralized control intelligence); or the EMD is a simple communication gateway in an open system that merely forwards signals from the external Smart Grid (decentralized control intelligence); or a hybrid model in which devices register limited information about their capabilities with the EMD and the EMD then interprets the Smart Grid signals before issuing its own control signals to selected devices (hybrid/distributed control intelligence).

The first scenario is a nightmare of never-ending software and firmware updates, since every time any vendor anywhere in the world creates a new device this knowledge must be put into every deployed EMD. Unfortunately it is also the most attractive from a vendor point of view, because closed proprietary systems are historically more profitable and faster to build.

The second is a fully decentralized system, essentially the Smart Grid signals are directly connected to every end-device (fridges, lighting, washing machines, etc.) and this device will make a decision about what action to perform when the Smart Grid sends updates. This requires more processing power in every device, and a standardized communication protocol between utility providers and end-devices. It also requires the user to setup every end-device so it will correctly decide what to do in every possible situation. The user interface issues with setting up devices that are all configured in different ways according to what the vendor felt like implementing, should not be underestimated. A prime example of the frustrations and waste this model causes can be seen in the number of remote controls for different electronic devices there are in most people's homes. It is doubtful that this model could survive long before some company made a local home aggregator, which brings us to the third model;

A more likely model is probably the hybrid model in which the user needs only configure the EMD, which will then control every other connected device. This provides a residentially centralized model in which a "home energy profile" of some description can be configured. However, it requires a standardized information protocol between the EMD and all devices so they can register their capabilities and how the EMD can control them. For instance, there must be a data format that can be exchanged between the EMD and all devices that specifies the type of device (for user-friendly identification), how much energy can be saved, the saving method (turn off or reduce consumption), and importantly how to send these signals to the device. A way for devices to report their energy usage to the EMD is also needed. The system must be designed for maximum flexibility and dynamic usage. The point is then that the EMD can interpret Smart Grid signals and issue control signals in the home network, e.g. when the Smart Grid reports an update on the price of energy, the EMD can decide that this is below its preconfigured threshold and can send start signals to the washing machine, heat pump, etc. Essentially informational signals are sent to the home/building EMD from the supplier and commandable signals are sent from the EMD to all local devices, which makes them all less expensive to build.

In general it can be said that it is preferable to have high-level control signals and then let the network sort out how to achieve this. For instance, the signals 'save 20% energy', 'maintain 19-21 degrees C', or 'shutdown' are high-level commands to a controller. A 'shutdown' might trigger a 30 minute process of halting the system, but the controller has the knowledge necessary to know how to perform a command on the system/device it is controlling.

Alternatively, with direct access to the devices it is easy to make control mistakes (e.g. tell windows to open, which will automatically turn the heat on a little later because it is cold). Giving such direct access to the device can be a bad idea, because it bypasses know-how and the system configuration. In some cases it is not even allowable, e.g. cooling counters in a supermarket. There are regulations about food safety, and cooling is a process that cannot just be turned on or off. A controller is needed in front of the system in order to decide what to do and how to do it.

Summary

There is a distinction between Commandable and Informational signals. Commands are direct control that can turn off or reduce the energy consumption of a device. Informational signals indirectly control devices by giving weather and price forecasts and then leave it up to some local control intelligence on whether or how to react to the information. Commands are better for simple embedded devices with low processing power; they can change modes, switch off, reduce energy according to a timer, etc. These types of devices typically sleep most of the time to conserve energy; they can have inaccurate clocks and be unreachable for periods of time. They can also be run on batteries and have wireless network connections.

Devices with higher processing power can better deal with informational signals. They can configure thresholds, calculate energy usage, activate or postpone some usage depending on price/weather, etc. They can also have storage space for calendars and have connectivity for clock synchronization, be directly connected to the Internet, obtain GPS info on where the user is currently located (and if anyone is on their way home), etc.

The Smart Grid command/informational signals must be agnostic about the transport method. There will inevitably be a variety of protocols and communication technologies that will pass the signal from the power supplier to the controller, each of which is optimal for the specific device or environment, or is simply traditional for that market segment to use (e.g. RS485, Ethernet, Modbus, ZigBee, M-bus, wired/wireless). These must all co-exist in a heterogeneous network[19]. Therefore all of them must work as a transparent transport layer (despite that some of the companies behind them wish to control the application as well), separated from the above Market Layer (as described earlier). This requires an addressing scheme at a high level of abstraction, which can eventually be translated into the appropriate address type used by the communication technology; in the same manner as the TCP/IP and DNS systems interact. There have been examples of systems where the address knowledge is in the wrong layer, e.g. using TCP/IP or ZigBee addresses in the application layer SOAP XML. This greatly limits the utility of the protocol and violates Separation of Concerns.

List of Communication Standards

What follows in this section is a list of different communication standards that are being used in the context of Smart Grid. These standards are not mutually exclusive; some of them deal with data transfer, some with storage formats, etc.

EnerNOC: Green Button[8]

This is a project to create an open format for Smart Grid data collection. It is maintained by the company EnerNOC, USA that is heavily involved in Smart Grid standardization. They create software for many aspects of Smart Grid, both calculation and management of risks as well as data logging and demand response.

EnerNOC: XMPP[12]

EnerNOC and other companies and research projects have experimented using the eXtensible Messaging and Presence Protocol (XMPP) for Smart Grid communication. The protocol is message-oriented and based on XML. It was originally named Jabber and many server implementations still retain this name. It is free and open (and several open source implementations exist) and was built for Instant Messaging (IM), presence information, and contact lists. The extensibility has meant that plugins for security, Voice over IP, video and file transfer, gaming, and other services were created later on. Due to the free and open-source nature of the protocol, it has enjoyed usage mainly as private enterprise-wide IM networks between employees. The security meant that messages could be sent across the Internet, and the open source meant that any IT admin could set up their own server and create an IM network. Google famously set up an XMPP to gTalk/GoogleTalk IM gateway server, which meant that any XMPP client could connect to the Google IM network.

EnerNOC used this protocol to create a system called PowerTalk, deployed in 2009, specifically for Smart Grid communication. The idea was that Smart Grid nodes, power stations, solar inverters, smart meters, wind mills, Energy Management Devices, and other devices that were part of the Smart Grid would simply act as IM users in a private XMPP network. These efforts have been continued by the company as they are standardizing XMPP as a high-performance transport mechanism in OpenADR2. In May 2013 they held a compatibility plug-fest in the OpenADR2 working group using XMPP between Smart Grid devices.

Other research projects[13] have looked into this avenue of communication as well, notably the Swedish Smart Grid initiative, which resulted in several extensions for XMPP (that are still in experimental/draft state), with focus on the Internet of Things (IoT). Among these, an Efficient XML Interchange format and standards for IoT Smart Grid sensor data, provisioning, control and concentrators.

Pros:

- XML based, which means it will be easier to transform to all the other XML-based Smart Grid initiatives.
- Message-oriented, presence detection and security are built in, as is a contact list. It is queue-like, some servers will store offline chats.
- Explicit identities (JID).
- The framework is extensible so new plugins can be made.
- Relevant extensions include the IoT XESs and a handful of plugins that manage sensor data, readouts, XML compression, etc.
- It is free and open source.

Cons:

- XMPP was designed for human to human messaging, not machine to machine.
- It was designed for one-to-one communication. Broadcasting is an afterthought (e.g. the PubSub extension), and quite necessary when e.g. publishing price forecasts to consumers in a Smart Grid.
- The contact list/roster and presence detection are really only needed one way: The utility provider is the only one who needs to check whether customers are online, so the provider would have an enormous contact list, whereas the customer would just have 1 contact. Managing the roster is also a challenge; the high number of presence updates provides a large overhead. A roster is also not an optimal way of managing automated clients. Extra security measures are needed to prevent clients sending and accepting invitations from each other, since this is what XMPP was built to allow. Disabling the roster essentially turns XMPP into glorified TCP connections.
- XMPP is not RESTful (ratpack is an HTTP over XMPP extension, but you might as well just use HTTP then).
- File transfer (as might be needed for weather forecasts or larger chunks of data) is also an extension.
- The security is not trivial to configure or manage.
- Apart from the useful services and plugins mentioned above, the protocol seems too over-engineered for the intended usage in Smart Grids, compared to a simpler RESTful interface.
- In summary, it seems that a good a piece of software used to create a prototyping example of a Smart Grid communication protocol for all the right reasons, has now become the actual protocol for all the wrong reasons. XMPP was used in some early research projects to show e.g. presence detection and XML data transfers in Smart Grid communication. Presumably the tool was chosen because it was free, open source, extensible, and had some of the services needed already built in. XMPP is a good demonstrator for these particular services and capabilities, but it should not be disregarded what the protocol was actually designed for (and all the other services that will be unused in a Smart Grid context), and it seems that trying to force the rest of the Smart Grid concept onto the protocol is not the best way to go about it. It would be better to find a more dedicated and purposefully designed protocol that had the same services, but none of the drawbacks, rather than trying to force the free

demo tool to actually become the finished product.

Alternatives to XMPP

It is worth having a look at messaging protocols that were specifically designed for machine-to-machine communication, but which so far have been overlooked by Smart Grid projects:

Advanced Message Queuing Protocol (AMQP)[15]

This is an open standard for message-oriented middleware. It is an application layer protocol and thus the standard mandates behavior that makes clients interoperable (whereas standardizing messaging middleware is often done at the API level, which does not ensure interoperability). It is meant for publishing data to many clients with focus on reliability and security. In particular it is designed for machine-to-machine communication and inherently supports one-to-one and one-to-many messages. It is used for cloud-based messaging (Windows Azure) and large file transfers. There is no roster management. It has RESTful interfaces (RestMS). There is offline message queuing and unique named queues. The protocol has payload fidelity, i.e. what is put into the queue comes out in the same order. The downside is that there is no built-in presence detection, however, presence is maintained via server pings in some implementations (nanite). There is no explicit identity, clients are instead bound to unique named queues and associated with them.

MQ Telemetry Transport (MQTT)[16]

Interesting is also MQTT; an open, royalty-free messaging protocol for machine-to-machine communication built for telemetry-style data transfer. It is suited for Internet of Things, i.e. small low-power embedded systems with high latency in constrained networks such as dial-up or satellite links. Design goals are simplicity in the API, compact binary payload, and it is ideal for push messaging such as temperature updates, oil pressure feeds, or mobile notifications. Devices range from sensors and actuators, to mobile phones, embedded vehicular systems, to laptops and PCs. It is an extremely lightweight publish/subscribe messaging transport with small code footprint and low bandwidth use. The particular focus on battery, bandwidth and reliability of message delivery makes this protocol interesting when looking at Smart Grid end devices, such as washing machines, heat pumps, temperature sensors, etc. The protocol is currently undergoing the standardization process at OASIS. Security is not built into the protocol, but it is designed to be tunneled via SSL/TLS.

Constrained Application Protocol (CoAP)[17]

CoAP is a software protocol under development intended for simple electronics devices to communicate over the Internet. It is particularly targeted for small low-power sensors, switches, valves, etc. to be controlled or supervised remotely. CoAP is an application layer protocol for use in resource-constrained nodes such as Wireless Sensor Networks. It translates easily to HTTP for simplified integration with the web, while also supporting multicast, very low overhead, and simplicity. There are two message types: requests and responses, using a simple header format. It uses UDP as default, but provides optional integration with DTLS (see below) for security.

Datagram Transport Layer Security (DTLS)[18]

DTLS is basically SSL/TLS over UDP. It provides similar security guarantees over UDP as SSL provides over TCP. The protocol is stream-oriented, but unlike TCP it has to deal with packet reordering, loss of data packets and data larger than a datagram packet size. It is supported by several open source library implementations, and is worth a look when trying to secure low-bandwidth UDP-based message protocols, such as the ones mentioned above.

OpenADR2[9]

OpenADR is the Open Automated Demand Response standard, which is basically the USA Smart Grid communication standard. A second version 'OpenADR2' is underway, offering a number of transport mechanisms, still under consideration[10]: SOAP, REST, HTTP, XMPP. Currently a sample REST-style HTTP is the only mandatory standard. It is a non-proprietary open standardized Demand Response (DR) interface that lets utility providers communicate DR signals to consumers.

The first version 1.0 offers only basic means of communication and has been used in the USA in local projects. It has also been tested in Canada, Ireland, France, Turkey, Spain, India, China, South Korea and Australia to a lesser extent. The ambition with OpenADR2 is to have a large ecosystem of vendors and to make it an International standard, offering test tools and certification programs[11]. The new framework will include informational signals for pricing, telemetry, and other services. The new standard will also mandate a security mechanism (TLS with certificates) and offer the option of higher security (adding XML signatures). There will be different device profiles, one for simple devices and one for complex devices, each requiring different levels of processing power and storage. Several projects began as part of the NIST Smart Grid initiative in 2009 to harmonize Smart Grid research in the USA, the outputs of which are used to define the OpenADR2 standard. It will be an international OASIS standard, and it is probably the closest to a Smart Grid communication standard at the moment. Other relevant OASIS standards include the EMIX (Energy Market Information Exchange) and EI (Energy Interoperation Standard). The downside is that the development is being driven by the USA and it is unclear whether it would translate directly into the systems already deployed and being deployed in the EU. Or why the EU is working on its own standard if OpenADR2 fulfills the same requirements?

Building Automation: BACnet, Modbus, KNX, LonWorks

These protocols are used in HVAC and building automation. They are not directly related to Smart Grid communication, but due to their status as the most popular protocols for Building Management Systems (BMS), they are often mentioned in relation to Smart Grids, since these are the protocols likely to be deployed in buildings to carry out the actual response to a demand signal from the Smart Grid. Presently there are no direct gateways between the protocols, but there are initiatives underway looking at these links.

KNX is a commercial open standard in the sense that vendors can create interoperable devices, but access to the standard itself and membership of the group is costly. Anyone can also create the controller chips. It is the successor of the European Home Systems (EHS) and the European Installation Bus (EIB/Instabus) standards. In practice there are only a few *de facto* producers of controller chips and not many vendors make similar or competing devices.

Modbus is perhaps one of the oldest surviving industrial communication protocols, invented in the 1970s. Its success is attributable to the industrial application focus, simplicity, flexibility of command and object definitions, and being openly published and royalty-free. It is often used in building automation, or industrial automation to connect networks of PLCs or SCADA systems. There are many limitations in relation to modern systems, such as restricted addressing space, lack of security, master/slave communication pattern, and lack of support for large binary objects. Nevertheless the sheer momentum of the many deployed installation of this protocol makes it relevant for any Smart Grid system, which must inevitably build on top of this network. For instance, the SunSpec Alliance that specifies the interoperability model of solar grid devices (inverters, smart meters, etc.) have standardized a Modbus object map for the different devices. Modbus can run over a serial bus RS485 (Modbus/RTU) or TCP/IP mediums (Modbus/TCP).

BACnet is a USA standard, widely deployed in building automation for HVAC systems. Like the other protocols it is openly published (but access and membership is expensive), royalty-free, and very flexible in terms of services and objects. The standard was first ratified in 1995; the latest version was published in 2012. It is suffering from an over-engineered abundance of datatypes, and the lack of progress in the 'application profile' workgroup has meant that new objects have been created in the standard for devices that should have just been a profile with a number of basic objects instead (e.g. rather than defining an Elevator or Security Door object with many properties attached, these devices should have been defined by a standard profile object map using basic binary and analog value objects instead of many properties on an object that only has one purpose). The standard defines a number of different transport mediums (RS-485, IP, ZigBee. LonTalk, ARCNET, Ethernet). It also defines how to combine BACnet networks with other technologies: a general non-BACnet network mapping, DARPA Internet Protocols, IPX, EIB/KNX, and WS Web Services Interfaces.

LonWorks (the platform on which LonTalk is a member) has long been a rival to BACnet and KNX, but some interoperability between them has been accomplished. It was created by Echelon for use over various physical mediums (twisted pair, powerlines, fiber, RF). It is mainly used in building automation and trains. It started as a closed, proprietary protocol[21] and the manufacture of the controller chip is done by Neuron, which is owned by Echelon (the implementation is also licensed to Toshiba and Cypress Semiconductor). In response to the success of BACnet, Echelon opened up the Lon standard in some senses by making the protocol public via various International standardization organizations. However, any LonWorks device must use the single-sourced Neuron chip, which is licensed along with the LonWorks software, design tools, and software development kit, all of which cost royalties. The design, marketing and absolute control of the technology is done by Echelon and no other companies or organizations have a say in how the standard will evolve, so for all intents and purposes it is still a closed, proprietary protocol. For this reason it is falling out of favor in some areas, which are switching to BACnet and/or KNX. Despite this it has a large install base and so must be considered when discussion building automation. One of the biggest criticisms is the long-term maintenance cost. Denmark bought many Lon installations for automating public buildings such as ministries, municipalities, courthouses, hospitals, schools, and the military. When these were due for an upgrade around 2010-2011, the projects had to be abandoned due to prohibitively high costs. It turned out that while the systems that had been bought may have had a lower acquisition cost than rivals, the costs of extending, changing, or replacing devices were disproportionality expensive. Especially the costs of new devices were very high, due to lack of competition in closed system and the licensing fees; but also the cost of simply reconfiguring the system since old software and systems had been abandoned and a costly upgrade of the BMSs were necessary. The military, which owns more square meters of buildings than any other public body, has had to institute a policy of acquiring only multi-sourced truly open systems (such as BACnet and KNX), in order to avoid future vendor lock-in of the magnitude seen in the hospitals and schools.

IETF

The Internet Engineering Task Force is developing a number of Internet protocols for the Smart Grid in RFC6272[14]. These are basically guidelines on how to use existing Internet standards for the Smart Grid, such as DNS, SSH, Kerberos, IPv4 and IPv6, etc.

European Smart Meter Communication Standardization Efforts

From the Smart Grid Communication Overview survey[19], the tables below show the EU standardization efforts as of 2011. These are mostly focused on Smart Meters since these are the focus area of current deployments in EU countries. Abbreviations: Smart Meter (SM); Gateway (GW); Home and Building Electronic Systems (HBES); Power Line Communication (PLC); Distribution Control System (DCS); Home Area Network (HAN); Wide Area Network (WAN).

	Connection between smart meters, devices, and displays	SM to SMGW	HBES (home automation network device, control, server, external server)	HBES to SM or SM-GW interface
Application	ZigBee Smart Energy 1.0/2.0, proprietary data model	CEN TC 294: EN 13757-3 MBus, CLC TC 13: IEC 62056 COSEM	CLC TC 205: EN 50090-3	CLC TC 205: EN 50090-3, CLC TC 13: IEC 62056 COSEM
Network and transport	ZigBee 2.0, 6LoWPAN	ZigBee 2.0, 6LoWPAN	CLC TC 205: EN 50090-4	CLC TC 205: EN 50090-4
Link and physical media	ZigBee, PLC, 802.15.4, Bluetooth, Proprietary protocols	CEN TC 294: EN 13757-2 M-Bus wired, CEN TC 294: EN 13757-4 M-Bus wireless, CLC TC 13: IEC 62056-31, Euridis 2	CLC TC 205: EN 50090-4	CLC TC 205: EN 50090-4

HAN communication and data exchange standards for Smart Metering in Europe

	SM-GW to Data Concentrator	Concentrator to DCS	SM-GW to DCS
Application	CLC TC 13: IEC 62056 COSEM	SMTP, SFTP, Web Service, COSEM	CLC TC 13: IEC 62056 COSEM
Network and transport	TCP/IP	TCP/IP	TCP/IP
Link and physical media	CLC TC 13 / IEC TC 57: IEC 62056 COSEM, DLMS/COSEM over IEC 61334/SFSK, PLC, GPRS and/or Ethernet/ ADSL	GPRS/GSM, PLC G3, Fibre VLAN, Point to multi-point radio	CLC TC 13 / IEC TC 57: IEC 62056 COSEM, DLMS/COSEM over GPRS

WAN communication and data exchange standards for smart metering in Europe

iPower Flexibility Interface

Not exactly a communication standard as such, but iPower is a consortium of Danish companies and research institutions collaborating on (among other projects) creating an end-to-end Smart Grid communication standard. They have published a Flexibility Interface[22] for modeling communication signals, particularly the Informational types of signals between aggregators, DERs and consumers. Pilot projects are being carried out in the working groups related to heat pumps, wind mills, and other supply and consumer technologies. The Flexibility Interface has a basis in IEC 61850 and attempts to standardize some of the data formats and types needed to communicate from the power substation to the different types of end-devices that would be included in a Smart Grid. The work done is similar to what OpenADR2 is working on.

Recommendations

In summary, a holistic Smart Grid standard does not exist and is not on the horizon yet. At the moment the OpenADR2 project appears to be the one with the most momentum and the one that has focus on a complete end-to-end communication solution, but it is being developed in the USA and it is unknown how well it fits the European ambitions of what the Smart Grid should be.

The Smart Grid concept encompasses such a vast range of products from different markets that have not traditionally been connected before, or indeed even had communication capabilities. Smart Grid communication initiatives have arisen in places where interoperability has become an issue, e.g. the SunSpec Alliance, but other than that companies are mainly implementing their own closed communication protocols for lack of an open one they can adopt.

For these reasons, our recommendation is to create an open, holistic Smart Grid interoperability communication protocol - in the sense that it is not specialized for a particular kind of product, application, or physical medium.

Requirements for an Open Embedded Smart Grid Communication Standard

To summarize the list of communication protocols in the previous section, there are a few trends and a few requirements that can be seen emerging from the different projects and their attempts at standardizing Smart Grid communication.

Basically, the only thing the world has agreed upon with regards to Smart Grid communication is the international IEC 61850-7 standard, which on the first page says “power substation automation”. Hence, the definition and scope stops at a high level in the power distribution model, long before an aggregator, end-user, or customer. The standard was designed for power substations in the USA. It has very complex models, objects, and data models for various devices and it is not suitable for embedded usage. In fact, as the SunSpec Alliance has learned, it does not define communication in sufficient detail for unambiguity. It is entirely possible to create two devices that fully conform to the standard, but which cannot communicate with each other. This is why the SunSpec Alliance is deciding on more details of the IEC 61850, in order to make devices interoperable, but their sole focus is on solar plants.

An ideal Smart Grid communication standard would be one that is basically a "light" version of the IEC 61850, i.e. a standard with more focus on embedded usage, less complex object and data models, and specified to a level of detail such that interoperability naturally follows. A focus on embedded usage means:

- A low-resource presentation of data. Binary XML, and less of it.
- Simplicity in implementation. Some sort of modular application protocol with device-specific services such that every device does not need to parse the whole language and be aware of every service and object in the standard. By implementing only what is necessary for a device from a modular library, the storage and memory footprint can be kept low. More resourceful aggregator devices, e.g. BMSs or EMDs can contain a full stack.
- Use of communication protocols specifically designed for embedded systems with low resource consumption (battery, memory) and low bandwidth (wireless networks, 6lowPAN). This is necessary because Smart Grid encompasses the home automation and building automation domains.
- Communication security must be an inherent part of the protocol, or at least be designed to wrap around it. Examples are DTLS (SSL via UDP) and certificate/key management, specialized Public Key Infrastructures.
- Research into the Internet of Things (IoT) and Wireless Sensor Networks, might be a good place to look for inspiration.
- Agnostic about application data so that it is not dependent on every device having the latest version. It is not the goal that every device should be able to communicate with every other device; the goal is that controllers can communicate with devices.

Roadmap for an Open Protocol

For the sake of argument we hereby refer to the: Seamless Protocol for Open Technologies (SPOT) as the open Smart Grid interoperability communication protocol.

If the open protocol SPOT were to be developed, it should be done in collaboration with universities:

- They know the trends of conferences and research in Smart Grid.
- They can bring together several interested companies and government funding.
- Development effort can be shared:
    - Developers from other companies.
    - Post-docs, master students, interns.

- They are very interested in use cases (requirements) from the industry; it strengthens their research credibility and relevance of their work.

Development of SPOT:

- Ensure that the protocol is agnostic about the application language being used, and use a Service-Oriented Architecture. That way different versions and different languages can co-exist in the same packet formats without requiring every device to support every version of every language. Several attempts at creating a Smart Grid standard have been abandoned because it was not possible to obtain a collection of descriptions of every possible device that exist or will exist in the Smart Grid. Therefore the protocol must be able to grow and adapt without fragmenting.
    - It is, for instance, conceivable to use the same packet format for heat pumps and solar inverters, even though none of them share functionality or services, or are able to communicate with each other (at least, in the first version of the protocol).
    - Subsequent versions may have messages that are interesting to both products, e.g. an energy price forecast.
    - A good service architecture will make it easy for devices to filter out packets that are not relevant for them at a low level, in order to spend the minimum amount of resources processing incoming packets. And also to set dynamic filters at runtime for messages that they are interested in.
    - This approach ensures that not every possible command signal of every possible product for Smart Grid must be defined in the standard before it can be implemented. As long as different services and versions can co-exist, the protocol is merely a communication bus, and the messages it carries can be extended dynamically.
- Interesting issues to investigate:
    - What should be the physical, MAC, transport layers? (Do we care at all?).
    - What commands should be used on the application layer, between which devices?
    - Is it possible to build every functionality of present (and future) devices by using simple objects (Analog, Binary values, Time, Schedules, etc.), and just defining which objects are to be used and what their functionality is, in application profiles? E.g. a heat pump has a profile stating which objects are mandatory and what they do. An electric car will have a different profile, but the objects will be the same. This approach has met some success in SunSpec and BACnet.
    - How to make a language that dynamically expands with full backwards compatibility when new types of devices are invented, new services are needed, and new objects are defined?
    - Security management. Particularly in regards to embedded systems with limited resources.

There are some immediate benefits to SPOT being used between communicating devices:

- Remote control/monitoring:
    - Differentiable interfaces, but based on same backbone.
    - Collecting usage information on stand-alone installations (heat pumps, food cooling,

HVAC, irrigation, etc.)
    - Internet connectivity: existing on-site LAN or GSM.
    - This is desirable functionality for many intelligent products at the moment, even if the vendors are not thinking in terms of Smart Grid connectivity yet. Several vendors have created their own cloud systems for their products to do this, but it is functionally equivalent to having a Smart Grid. At the moment the clouds just are not connected.
- Cloud-based Smart Grid access. Connecting through servers gives the following opportunities:
    - Monitoring of customer data (by permission) enables data-mining of how products are used, how energy efficient they really are, how often and why they fail.
    - Immediate support access via Internet
        - Direct trouble-shooting of system.
        - Access to configuration settings and setup information.
    - Network security:
        - Address resolution
        - STUN server capability (NAT/Firewall traversal)
        - Access management
        - Secure device pairing

System Overview with a Cloud server

The immediate issues of the lack of a communication standard in Smart Grid and the opposing requirement of being able to have products that communicate with the Cloud, point to a solution in which the Cloud is isolated from external influences such that implementing a standard at a later time incurs minimal development costs (i.e. not having to firmware upgrade every deployed product at every customer site).

For some ideas on 'future-proofing' the Cloud, see figure 1 below:

- Connection from the product to the Smart Grid goes via the Cloud.
- New standards and protocols require minimum effort to incorporate, just write a new plugin and host it in the Cloud.
    - **When/if the EU, USA, China, Japan, and India finally decide on each their own versions of a Smart Grid communication standard, the rest of the communication path is not affected.**
- The proposed Cloud is WEB/XML/HTTP/REST-based, which is the current trend of Smart Grid specification models and protocols, so there is little risk that upcoming standards will be fundamentally incompatible with this proposal.

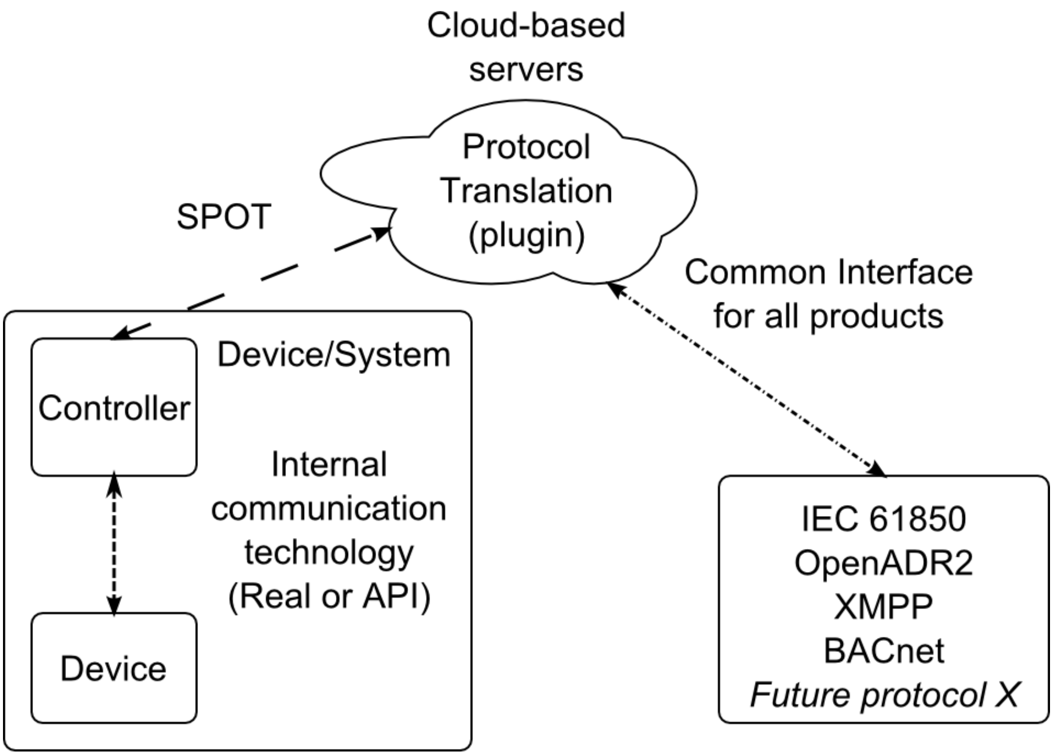

Figure 1, Cloud-based separation of SPOT and various external standards

The above figure 1 shows the Cloud from the perspective of the external world. The box on the far right contains standards that we cannot influence or control, but we will have to implement. This box of uncertainty and change is to be kept in front of the cloud, and the cloud presents a common interface to the user for all products, regardless of the external standard being used. The cloud can do translation between the external standards (the environment of dynamic communication standards) and SPOT (the environment of static communication standards). When new external control standards appear, it is a (comparatively) simple matter to write a new plugin for the cloud and then every device already deployed will be able to use that standard without necessitating a software upgrade on the device. Since the connection from the device to the cloud may be lost, this model works for non-critical systems. Behind the cloud is the SPOT protocol linking the cloud and the device/product. The product consists of a controller that contains the control intelligence of the system (e.g. how to control a cooling or heating process), and the device itself. In some cases this distinction is physical: a thermostat attached to the radiator (device), a touchpad on the wall (controller), and internal communication via a wireless technology or serial bus. In other cases both are built into the same physical box and the distinction is only logical via an API. For some systems the Cloud functionality can be built into the device either as redundant backup, or as main location (see the discussion on Control Intelligence in previous sections).

Figure 2 below shows the same picture, but from the perspective of what SPOT can be used for. The external box on the right shows capabilities that are desirable for Smart Grid products to have or to offer to customers, which can be implemented in some external device (dedicated embedded devices, smartphone, laptop, etc.). The device on the left and SPOT are the same as before; however, since the devices use SPOT to communicate with the Cloud, they can also be directly communicated with by the external devices on the right (Direct Control), if these devices also use SPOT. This enables their usage for critical control applications as well, since the cloud and Internet can be bypassed. In this case the Cloud Control is a Cloud redundant backup instead, or a bulk transfer channel for accumulated logs (passive data capture). This enables non-real-time logging (via Cloud) together with real-time control/monitoring (bypassing Cloud).

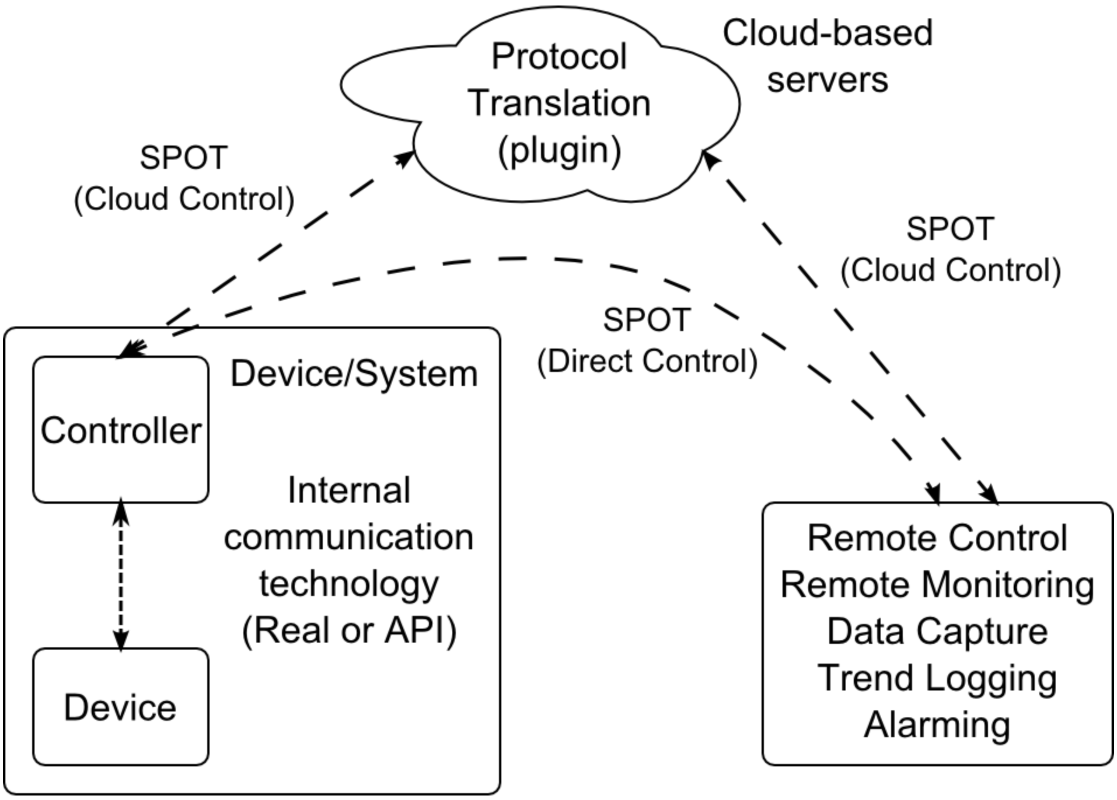

Figure 2, SPOT used as both direct control and cloud control protocol

The security model for the protocol is based on the Cloud managing the remote pairings of devices and remote controllers (e.g. Smartphones, web interfaces). This is similar to the roster management of Instant Messaging networks mentioned previously. This way, devices can define their own virtual subnetworks of trusted peers over the Internet - basically like a small VLAN/VPN, but with simpler implementations that do not require as much overhead of processing power of embedded systems. Mainly because the application does not require a constant TCP connection and network sharing - the only requirement is to send occasional control commands or status requests from a remote device. There is simply a registered ID pairing between devices and remote controllers stored in the Cloud and the Cloud maintains an open connection (like a STUN server). Cryptographic proofs of IDs provide authentication both between the device and the Cloud, and between devices. The encryption and authentication algorithms are handled by standard protocols, e.g. SSL, OAuth, XML-Enc, etc.

References

1	http://www.danskenergi.dk/~/media/Smart_Grid/Smart_Grid_Rapport.pdf.ashx
2	http://ses.jrc.ec.europa.eu/jrc-scientific-and-policy-report
3	http://ses.jrc.ec.europa.eu/assessing-smart-grid-benefits-and-impacts-eu-and-us-initiatives
4	http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCoSStandardsInformationLibrary
5	http://ses.jrc.ec.europa.eu/sites/ses/files/documents/smart_grid_projects_in_europe.pdf
6	http://ses.jrc.ec.europa.eu/sites/ses.jrc.ec.europa.eu/files/documents/ld-na-25815-en-n_final_online_version_april_15_smart_grid_projects_in_europe_-_lessons_learned_and_current_developments_-2012_update.pdf
7	http://www.sunspec.org/
8	https://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/GreenButtonSDK http://open.enernoc.com/data/
9	http://en.wikipedia.org/wiki/Open_Automated_Demand_Response http://openadr.lbl.gov/ http://drrc.lbl.gov/projects/automation-communication http://drrc.lbl.gov/system/files/LBNL-5273E.pdf
10	http://cio.nist.gov/esd/emaildir/lists/h2g_interop/pdf00009.pdf
11	http://www.pointview.com/data/2012/05/55/pdf/Rolf-Bienert-ISAEHDDT-16182.pdf
12	http://open.enernoc.com/ http://www.smartmeters.com/the-news/521-enernoc-launches-powertalk.html http://www.greentechmedia.com/articles/read/enernoc-building-the-big-data-platform-for-demand-response
13	http://wiki.xmpp.org/web/Joachim_Lindborg_Application_2013 http://wiki.xmpp.org/web/Tech_pages/IoT_XMPP_Process http://iea.sust.se/2013/04/18/265/
14	http://www.rfc-editor.org/rfc/rfc6272.txt
15	http://www.amqp.org/ http://www.rabbitmq.com/ http://blogs.vmware.com/vfabric/2013/02/choosing-your-messaging-protocol-amqp-mqtt-or-stomp.html
16	http://mqtt.org/
17	http://tools.ietf.org/search/draft-ietf-core-coap-18 http://en.wikipedia.org/wiki/Constrained_Application_Protocol
18	http://en.wikipedia.org/wiki/DTLS http://tools.ietf.org/html/rfc6347
19	http://arxiv.org/abs/1112.3516
20	https://www.eff.org/nsa-spying/nsadocs
21	http://www.stitcs.com/en/lonworks/bacnet%20vs%20lonworks.pdf
22	http://www.benjaminbiegel.com/flexibility-interface-%E2%80%93-information-modeling-for-direct-control-84.html

Appendix

The following is a list of Smart Grid projects that have included some form of Smart Grid communication. All information is taken directly from appendices of [2] and [3], see these for more information:

internet of energy NO

The objective of Internet of Energy (IoE) is to develop hardware, software and middleware for seamless, secure connectivity and interoperability achieved by connecting the Internet with the energy grids. The project will evaluate and develop the needed ICT for the efficient implementation in future smart grid structures.

LINEAR BE

LINEAR project is a first crucial step in the transition towards smart grids in Flanders. The project focuses on the realization of a technological and implementation breakthrough by innovative technological research and a large scale pilot in a residential area. This will be achieved in close collaboration with industrial partners and associated Flemish innovation platforms. Scope of the project: installing of distributed energy sources and load management at 1000 clients within the smart metering project in Hombeek and Leest

more microgrids EL

The aims of this Test Facility is to: ? Test centralized and decentralized control strategies in grid interconnected mode; ? Test communication protocols and components including aspects related to energy trading; ? A control and monitoring system built around IEC 61850 standard designed and prototyped; ? Control strategies resulting from agent software to make use of these control and monitoring functions; ? Development of intelligent modules embedding the required functions to allow a full integration of each generating/load unit into the system

nextgen DTU DK

To contribute to the development of next generation communication system for system integration of distributed generation (NextGen) based on the new international IEC61850-family of open standards developed in these years.

open node ES

OpenNode project is focused on the electrical distribution grid operation and explores answers on the three challenges introduced: ? How to improve the distribution grid monitoring to cope with volatile states in the grid ? How to integrate the gsmart h substation automation devices to increase the efficiency of the distribution grid ? How to interoperate with the different roles e.g. operation of the smart meters, power and grid operation

Real-time demonstration test and evaluation of Bornholm electricity network with high wind power penetration

DTU DK

Create a research platform, where elements of future the energy system can be tested. Testing can be performed from the laboratory level and up to full scale demonstration on Bornholm.

Second1 - Security concept for DER

EURISCO DK

The project objective is to analyze and implement a security concept that can be used in a power system with a high degree of decentralized production and with many actors in an unbundled market. It will also investigate various forms of role based access control (RBAC).

Smart watts DE

The Smart Watts projects implements the concept of the ?smart watt e, i.e. the intelligent kilowatt hour: an open system, which enables new services, value added and increased efficiency for utility companies, device manufacturers, service providers and consumers.

smart grid web AT

Future smart grids will rely on data exchange between different applications and market participants. Smart Web Grid analyzes user interaction, technology, cost effectiveness and data security of such a data exchange by means of three concrete examples in the model region Salzburg. The goal is the conceptual design of an information model for Web service-based access to smart grids data sources.

STAmi IT

The project aims at developing a dedicated application for LV network management and business purposes which leverages the existing metering infrastructure. STAmi provides network operators with a dedicated web interface to collect, on demand and real-time, specific high quality and accurate data stored in smart meters without additional load for the Advanced Meter Management (AMM) system. Both the operators in the control room, in the back office and on field work operators (via tablet PC) are provided with a dedicated suite of functionalities and tools based on web interfaces.

Storstad smart metering SE

Echelon fs Network Energy Services system provides E.ON with an open, bidirectional, and extensible infrastructure that enables a comprehensive range of utility applications that brings benefits to every aspect of their operation, from metering, to customer services, to distribution operations, to value-added services.

SmartHouse/SmartGrid DE

The SmartHouse/SmartGrid project sets out to validate and test how ICT-enabled collaborative technical-commercial aggregations of Smart Houses provide an essential step to achieve the needed radically higher levels of energy efficiency in Europe.

smart grid demonstration system UK

Arqiva will use its dedicated UHF spectrum, combined with Sensus f purpose designed security measures, to provide a bespoke communications network for independent use by the UK fs water, gas and electric utilities

Plug n f play-concept for

intelligent indeklimastyring, ForskEL Neogrid DK A concept for energy efficient control of air-air heat pumps and electric storage water heaters with focus on indoor climate, energy savings and demand response is developed.

fenix ES

The objective of FENIX is to boost DER (Distributed Energy Resources) by maximizing their contribution to the electric power system, through aggregation into Large Scale Virtual Power Plants (LSVPP) and decentralized management. The project is organized in three phases: ˜ Analysis of the DER contribution to the electrical system, assessed in two future scenarios (Northern and Southern) with realistic DER penetration; ˜ Development of a layered communication and control solution validated for a comprehensive set of network use cases , including normal and abnormal operation, as well as recommendations to adapt international power standards; ˜ Validation through 2 large field deployments, one focused on domestic CHP aggregation, and the second aggregating large DER in LSVPPs (wind farms, industrial cogeneration), integrated with global network management and markets.

From wind power to heat pumps DK

energinet.dk

Tto control 300 intelligent heat pumps as if they were one big energy storage facility capable of storing electricity as heat.

Heat Pumps as an active tool in the energy supply system,

ForskEL

Heat pumps will provide flexibility due to the possibility to either increase, decrease or interrupt the power consumption. The project will deal with the ability of heat pumps to operate in so-called Virtual Power

Plants, to deliver regulating power and to react on spot-market electricity prices.

Elforsk smart grid programme SE

Elforsk Smart Grid Program is driven as a national programmer for four years with financing and participating from Swedish utilities and other companies. A common steering group takes decision for each project/ sub project in the program. The normal delivery from a project will be an open report available for all participants and normally also put on internet as a public document. The program will also interact with other large pilot projects as Stockholm Royal Seaport with Fortum and ABB and Gotland Smart Grid project with Vattenfall and ABB

energy@home IT

Energy@Home project aims to develop a system in which gsmart appliances h can manage themselves by adjusting power consumption depending on power supply and prices, or in order to avoid overloads within the house. In addition Energy@Home provides information to the user, such as power consumption of appliances, hourly cost of energy, green level of the energy being supplied; this information is made available on the user fs PC, mobile or on the display of the appliance.

address IT

The project aims at delivering a comprehensive commercial and technical framework for the development of gActive Demand h in the smart grids of the future. ADDRESS investigates how to effectively activate participation of domestic and small commercial customers in power system markets and in the provision of services to the different power system participants.

ecogrid EU DK

To build and demonstrate a complete prototype of the future power system with more than 50% renewable energy. The primary focus is on market integration and inclusion of electricity customers in the building of tomorrows Smart Grid. Eco-grid eu, bornholm. pv, ev, heat pumps

ipower 2016 DK

The goal of the platform is to contribute to the development of an intelligent and flexible electricity system capable of handling a large part of sustainable electricity production in areas where production varies due to weather conditions (sun, wind etc).

openmeter ES

The main objective of the OPEN meter project is to specify a comprehensive set of open and public standards for Advanced Metering Infrastructure (AMI) supporting multi commodities (Electricity, Gas, Water and Heat), based on the agreement of the most relevant stakeholders in the area.

miracle DE

The project fs main goal is to develop a concept for flex-offers that specify electricity demand and supply which is flexible in time and amount and an infrastructural approach to process lots of these flex-offers issued by small consumers and producers in near real-time. The possibility to shift demand within the mass of households developed within the MIRACLE project will allow for a higher share of fluctuating renewable energy sources in the energy mix on the grid and reduce the peak demand. We expect that the share of RES can be increased by 5% and that the peak demand can be reduced by 8-9% (but at least by 5%) for the total grid. We will furthermore reduce the mean time between transactions, which will result in more stability of the energy grid but also in reduction of costs of BRPs, by reducing the difference between their planned and actual electricity schedules

optimate FR

The project aims at developing a numerical test platform to analyze and to validate new market designs which may allow integrating massive flexible generation dispersed in several regional power markets.

DataHub project 2009 2012 Energinet.dk

http://www.energinet.dk/EN/El/Datahub/Sider/DataHub.aspx

A more free competition in the Danish electricity market, easier access to information and more transparency for consumers who choose to switch supplier. A desire for more standardised communication between players on the Danish electricity market

READY ? Smart Grid ready VPP controller for heat pumps

2012 2014 Nordjysk Elhandel n/a

The aim is analysing, developing and demonstrating a smart grid ready Virtual Power Plant controller that includes the complex challenges of large scale demonstration with demand flexibility, balancing possibilities, grid constraints, optimising across a pool of heat pumps, house models, user comfort, acceptability and business models.

TotalFlex 2012 2015

Neogrid Technologies, Denmark

http://www.totalflex.dk/In%20English/

TotalFlex is a demonstration project that intelligently manages flexible consumption and production. This is done by flex-offers from a technical and commercial VPP, which are traded on a marketplace. Thereby the full flexibility is utilised in an optimum way, while power-balance-liability and network capacity is taken into account.

Greenlys 2012 2016 ERDF http://www.greenlys.fr/

GreenLys is a systemic smart grid project which includes: ? DER ? Consumption ? Networks (DSO & TSO) Main Goals: ? decrease of greenhouse gases ? control of energy bill ? introduction and control of DER on LV networks ? behaviour of consumers, with incentive and innovative new offers ? aggregator functions Innovations: ? Smart management of grid (seal-healing, smart metering using Linky infrastructure,...) ? Demand Side Management, Demand/Response, energy saving and new offers (using boxes linked to Linky Infrastructure, tariffs, dynamic prices policy...) ? Investments, Impact on studies and development of networks (especially for DSOs)

REFLEXE:

Electric Flexibility Response for Smart Grids 2010 2013 Veolia Environnement

http://www.veolia.com/en/medias/pressreleases/reflexe.htm

The Reflexe project consists in implementing a smart grid pilot in France fs Provence- Alpes-Cote d fAzur region. The new electric grid will integrate many diverse and widespread sources of decentralised generation, storage and consumption. It will therefore have to manage considerable amounts of information in real time using a communication network in parallel. As the link between electricity producers and consumers, eenergy aggregators f will have the role of monitoring in real time all local installations in order to produce locally, store power and supply it to the grid as required.

MODELEC:

optimiser la gestion des usages electriques residentiels 2012 2014 Direct Energie

This is a pilot project on the behavioural adoption of Energy Efficiency services and Demand Response programmes over 1 000 homes in France. The project proposes to examine customers f behaviour in situations of peak demand where additional fossil fuel generation sources used. The interest is to shift some consumers use during peak periods to limit the use of carbon sources of energy. Precise knowledge of the customer fs consumption, accompaniment through tools and tips to automatically control some equipment and to change their behaviour, give them the means to minimise their overall annual consumption.

MILLENER:

control demand of individuals and improve the integration of renewable energies in the islands. 2012 2016 EDF

http://investissementavenir.gouvernement.fr/content/l%E2%80%99etatengage-28-m%E2%82%ACpour-desprojetsr%C3%A9seaux-electriquesintelligents-smartgrids

The research project MILLENER aims to reduce the electricity consumption of customers and to better integrate intermittent renewables into distribution networks in order to ensure real-time the balance between electricity demand and production. It takes into account the specificities of a non-isolated network interconnected, such as islands, and the need to educate users to control their consumption. These experiments will consist of facilities photovoltaic panels, energy storage systems and control of electrical consumers.

Netze der Stromversorgun g der Zukunft 2008 2011 RWE DAG

http://www.rwe.com/web/cms/de/683570/smartcountry/

One of the most promising investigated grid structures will be demonstrated in a typical rural MV grid, which has to cope a massive implementation of RES. Several technologies like electronic sub-stations, automatic tap changer, the usage of the flexibility of a biogas plant etc. will be tested and demonstrated. Three components are tested in the course of the model project: newly developed voltage regulators for protecting against voltage fluctuations, recording and communicating real-time production and consumption data, and using biogas storage to compensate for peaks in supply and demand

Yello Sparzahler online 2008 2009 Cisco

http://newsroom.cisco.com/dlls/2009/prod_100509e.html

Project aim is to create an intelligent energy system that allows customers to measure and control the power consumption of their electrical appliances, enabling them to reduce their monthly bills. In the current pilot, 70 homes and businesses have been selected to communicate intelligently with the local power grid and power sources over an Internet Protocol network. Customers can use Yello Sparzahler online to receive information about their electricity consumption in real time while, a home energy management system also allows them to set appliances to operate during offpeak periods

DESI ? (Pervasive Energy-Sensitive ICT Production)

2011 2013 Deutsche Telekom AG

http://www.desiit2green.de/

DESI aims at introducing load-adaptive mode into Telco network operation. In utility lingo, this turns a Telco network into a large consumer with demand-response capabilities. Furthermore, the UPS systems integrated into the network contain considerable energy storage capacity which is rendered accessible to smart grid use cases. A unified control framework as it is developed within DESI provides the communication infrastructure to impose complex optimisation algorithms onto load and storage management.

Energy @ home 2009 2013 Enel Distribuzione SpA www.energy-home.it

eEnergy@Home f project aims to develop a system in which esmart appliances f can manage themselves by adjusting power consumption depending on power supply and prices or in order to avoid overloads within the house. In addition Energy@Home provides information to the user such as power consumption of appliances, hourly cost of energy, green level of the energy being supplied; this information are made available on the user fs PC, mobile or on the display of the appliance. Installation in residential homes of Energy@home system (Enel Smart Info, Telecom Gateway, Smart washing machine, Smart plugs, Application tools). It allows continuous real-time bidirectional information exchange between on one side utility, retailer, telecom and manufactures and on the other side appliances and energy generation plant in the houses