EXPERIENCES FROM NORWEGIAN SMART GRID PILOT PROJECTS

Kjell SAND
SINTEF Energy Research/NTNU,Norway
kjell.sand@sintef.no

Dag Eirik NORDGÅRD
SINTEF Energy Research – Norway
dag.eirik.nordgard@sintef.no

Tarjei Benum SOLVANG
Nordlandsnett - Norway
tarjei.solvang@nordlandsnett.no

Jan FOOSNÆS
NTE/NTNU – Norway
jan.foosnaes@nte.no

Vidar KRISTOFFERSEN
Fredrikstad Energinett – Norway
vidar.kristoffersen@fen.no

Dagfinn Wåge
Lyse - Norway
dagfinn.wage@lyse.no

ABSTRACT

This paper describes results from three on-going Smart Grid pilot projects within the Norwegian Smart Grid Centre. The paper provides and experiences from the first phases of the pilot projects, including Smart Meter roll-out, verification of different communication technologies and challenges regarding ICT security.

INTRODUCTION

The development and deployment of Smart Grids technologies and solutions is gaining momentum all over the world, supporting the vision of a sustainable and reliable future energy system. Norway has started to implement Smart Grids as the regulator (The Norwegian Water Resources and Energy Directorate -NVE), adopted on 24 June 2011 new rules providing for the large-scale deployment of Smart Meters to be 100% completed by Jan. 1st 2017. As Smart Metering is a key-enabling technology for Smart Grids, it is fair to state the Smart Grid evolution in Norway is in the pipeline. This decision is on the top of the agenda of the DSOs (Distribution System Operators) and as the development will take place several years earlier than most of Europe (80% by 2020, 100% by 2022), the seek for standardized, robust solutions fulfilling the functional requirements of the regulator is urgent. It is thus important to create a good knowledge base for strategic decisions including Smart Grid strategies beyond the most eminent requirements.

To prepare for the challenges regarding Smart Grids development and deployment, the Norwegian Smart Grid Centre (NSGC) was established in 2010. The NSGC is an association with 50 members from trade, industry, education and R&D. The goal of the centre is to contribute to a safe, efficient and environmentally friendly energy system providing better utilization of the electricity supply grid and increased use of renewable energy sources.

In order to gain experience with Smart Grid technologies, the NSGC is focusing on establishing laboratories and large-scale demonstration sites, which will make a significant contribution to both research and education, and also provide opportunities for the industry and suppliers to test their products under realistic conditions. The NSGC is therefore contributing to the development of national demonstration sites for Smart Grids technologies for common experience and learning.

Three Smart Grid demo sites have been established within the NSGC:

- Demo Steinkjer
- Smart Energy Hvaler
- Demo Lyse

The demonstration sites are located in different geographical regions, managed by local DSOs and having different areas of focus. By sharing information and results, the purpose is to reduce the risks related to the significant investments which will be made in the years to come.

The three pilot projects are well underway and have already completed important parts of the first phases. This includes Smart Meter roll-out, with different communication technologies and analyses of ICT systems and security. Through these processes both challenges, use cases and potential benefits are identified.

SMART METERING REQUIREMENTS

The Regulations set that, by 1 January 2017, all customers in Norway must be equipped with smart meters. From the Norwegian Regulator's point of view, Smart Metering technology is evaluated as an enabler for a more efficient power market, a more optimal consumption of electricity and good management of the power systems.

The Regulator has specified the following objectives for the implementation of Smart Metering technology [1]:

- Exact billing of the electricity consumption
- Easier to change power supplier
- Increased competition between the power retailers, and thereby reduced prices and new products/services
- More efficient control of the distribution system
- Increased information to the customers regarding prices and their electricity consumption.

The costs related to full-scale deployment of Smart Metering technology in Norway are estimated to 10-12 bill.

NOK including communication and back office software systems (1€=7,5 NOK). The following functional requirements to the new smart meters are specified in [1]:

The smart meter shall…

a) *Store the meter data with a registration frequency of maximum 60 minutes. It should be possible to change the registration frequency to minimum 15 minutes*
b) *Have standardised interfaces that adjust for communication with external equipment (e.g. customer appliances) based on open standards)*
c) *Be able to connect different types of meters (gas, heat, water, …)*
d) *Secure data storage at voltage outages*
e) *Disconnect or reduce (electrical fuse) the total load at the customer, except for customers metered at distribution transformer level (larger customers)*
f) *Be able to send and receive price information (energy contracts and network tariffs) and signals for load control and earth faults*
g) *Give security against misuse of data and unwanted access to load control functionalities*
h) *Measurement of both active and reactive power – in both directions – four quadrant measurement*

Hourly meter data shall be:

- *Stored in the meter until transferred to the DSO*
- *Transferred to the DSO after the end of the day*
- *Available for the customer and the power retailer within 09:00 the next day*

SMART METER ROLL-OUT

In the three pilots, a total of ca. 10000 Smart meters have been deployed of different types and with different communication technologies. An example of the infrastructure is shown in Figure 1.

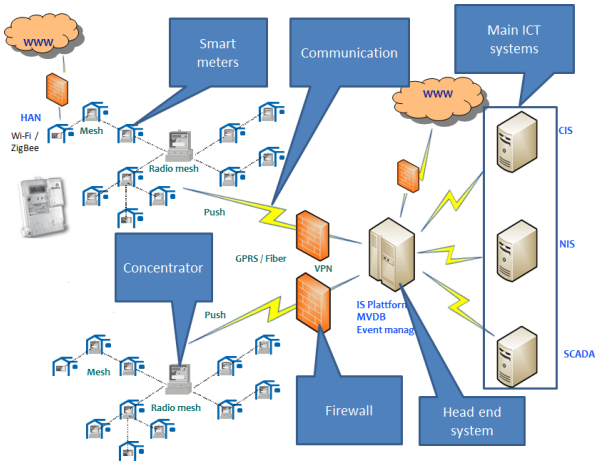

Figure 1 Smart metering infrastructure at Hvaler Island

Technology and features were selected to meet Norwegian requirements for smart metering.

In two of the pilots Radio Mesh (RM) technology has been applied with a two-way communicating mesh network at frequencies 433-444 MHz or 868 MHz . All meters act as nodes in the network receiving and forwarding data and operating independently from one another. If a meter is removed, the network will automatically re-route the data communication. When added to a network, a meter will automatically assist in routing communications.

The radio frequencies applied is in a range where radio signals easily penetrate buildings, travelling through windows and walls.

In one of the pilots, the fiber-to-home communication has been applied. As several DSOs in Norway belongs to companies that also have telecom operations based on this technology, it is of interest to use this already established communication link for Smart metering data.

The experience from the roll-out has identified some factors to be important for successful roll-out:

- *Sufficient planning*. It is important to commit substantial resources in the planning phase involving all internal stakeholders to avoid ad-hoc decisions and solutions in the roll-out phase.
- *Well documented and tested roll out processes*. There are many sub processes during the roll-out and each one of them should be well established and tested thoroughly prior to start of roll-out. Each process must be communicated to personnel participating in execution of the processes. It is also important to define what the electricians are allowed to do/ not to do during roll-out to avoid communication with customers outside the scope of DSO operations (e.g. promote electricity sales which is outside the scope of the DSOs)
- *Communication with the customer*. To have a proactive information process with the customers is important to create goodwill and understanding for the new technology to be deployed. Thorough and extensive customer communication process in the smart meter roll out pilot projects resulted in motivated and positive customers. This secured a high hit rate when the electricians came at the scheduled time to replace the meters.
- *Roll-out ICT support*. To have a proven ICT tool for field operation supporting all tasks to be performed and well integrated to the Customer Information System is very important. When there is a lack of proper addresses and/or the electricians are not familiar in the area they are working, the field tool and work order management system need good support for map functionality and coordinates. Good support for recording deviations is also important. Documentation by

pictures before and after Smart meter installation is recommended.

- *Quality assurance from day one*. During the first phase of the roll-out it is important to have close follow-up on each electricians to make sure they are performing the tasks correctly and that they record all necessary data. The DSO must make sure that the person/company responsible for the roll-out and the electricians are committed to and follow-up all obligations in the roll-out contract to avoid tempting cost saving short cuts to be take resulting in reduced quality.

COMMUNICATION ARCHITECTURE

A central part of the first phase of the pilot projects is to test different communication technologies and systems to create a knowledge base for selecting the most suitable technologies for full scale implementation. The focus has been on the communication from the Meter to the Head-End System (HES). In the tested infra structures the communication path can be "directly" from the meter to the HES or via a concentrator or gateway/home terminal. Typically a concentrator serve as a hub for a number of meters and the concentrator might also have the capacity to serve as a smart meter. Thus, two main links might be necessary to push or pull data from the Meter to the HES. In radio mesh systems; there will also be data traffic between different nodes (hops) in the radio network before reaching the concentrator. The situation is shown in Figure 2. Table 1 shows examples from response time test for different configuration and technologies.

Table 1 Response time smart meter single data request

	Technology		**Time (sec.)**
Meter→ HES (P2P)	GPRS		10-30
	EDGE		8-30
Meter→ Concen-trator→ HES	**Technology Meter-concentrator**	**Technology Concentrator - HES**	
	RM433MHz 1 hop	GPRS	7
	RM433MHz 2 hops	GPRS	8
	RM433MHz 3 hops	GPRS	9
	RM433MHz 4 hops	GPRS	11
	RM 868 MHz	GPRS	30-35
	RM 868 MHz	EDGE	12-15
	Wifi	Fiber	< 2

The single smart meter data request illustrated in the table might be relevant when dealing with a customer telephone inquiry and the DSO representative wants to check meter data e.g. present voltage level or alarms. The timings shown in the table should all be acceptable for such a customer management use case.

Communication testing has revealed several practical issues:

- Radio mesh systems might have variable performance and some smart meters might be difficult to reach without extra antenna
- Wireless communications depending on third party availability and performance is an issue
- Using external telecom provider solutions should consider that technologies and standards in telecom changes more frequent than in the power system business.

During the various tests performed, system integration and interoperability challenges have been identified do to the lack of standardized interfaces between the systems involved in the information chains shown in Figure 2. To obtain a cost-efficient information infrastructure, it is imperative that standardized interfaces are used to avoid the need for system vendors to tailor integrations which might be costly and need to be maintained over time.

ICT SYSTEMS AND SECURITY

A high-level identification of information security threats of the AMI pilot in Demo Steinkjer have been investigated primarily concerning the smart meter and its communication with the head end system of the Distribution System Operator (DSO) – see Figure 2 for more details see [2]. The Home Area Network was out of scope.

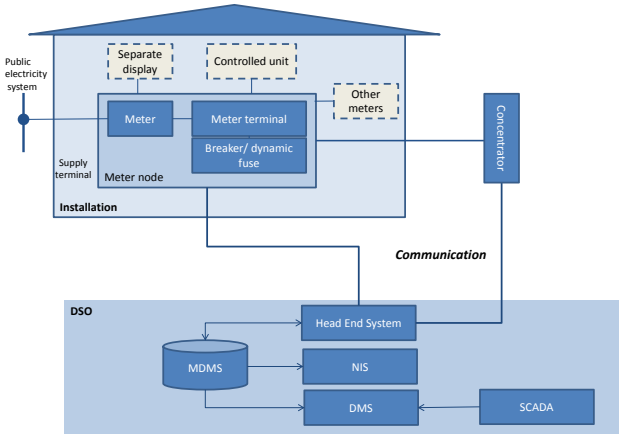

Figure 2 AMI Infrastructure and system interfaces

The risks related to the introduction of smart meters in Demo Steinkjer are addressed from two angles:

- **Threat overview and identification**: To ensure a high coverage of threats, a structured method to identify threats on the possible attack interfaces is used. The information flow of the AMI system is described using Data Flow Diagrams (DFDs) and the trust boundaries are identified. Then, for each trust boundary, the relevance of the STRIDE threat categories is assessed. This method is based on the threat modelling approach of Microsoft [3].
- **Attacker goals and strategies**: The important assets of the system are identified and by investigating the system using the approach given in [4]. Then attack goals are associated with these assets, and the possible ways to achieve the goals are detailed in attack trees [5].

The high-risk incidents comprise one or more of the following:

- Unwanted power outage for several customers
- Software flaw
- Head End System at utility company fails or is used in the attack
- Internal personnel misuse knowledge and/or legitimate access

The threat analysis of Demo Steinkjer focuses on threats that come from the meter side, thus the two last incident types are not covered in this study. The main attention is also on malicious acts.

30 threats have been identified for the different interfaces analysed – see Table 2

Table 2 Threats identified

STRIDE category	Master meter-HES	Master meter – slave meter	Meter-3rd party equip.	Meter-local maintenance interface
Spoofing	2	1	0	1
Tampering	1	2	0	2
Repudiation	2	0	0	1
Information disclosure	2	2	1	0
Denial of service	3	3	1	2
Elevation of privileges	2	0	0	1

Identification of threats is an important step in understanding the risks of a system, and evaluating whether a system is adequately protected. When threats have been identified, it is however necessary to assess the system's level of vulnerability towards the threat, and also the potential consequences of a breach. Full risk analysis details cannot be included, as this would violate confidentiality agreements with vendors and DSOs.
The study only identifies threats, but do not prioritise them and also do not suggest how to mitigate them. The aim of the study has been to better understand the threats facing AMI systems. Understanding is the first step, but needs to be followed by wise decisions and actions.

CONCLUSIONS/FURTHER WORK

The lessons learnt from the pilot projects so far shows that it is important to carry out such projects to get good quality in the large scale implementation of smart meter and smart grid technology roll-out. It is better to do mistakes in a small scale. Many of the issues and experience gained are of quite practical matter and thus not easy to reveal in a more theoretical approach. Tested communication infrastructures normally work well with adequate response times, but local communication availability issues have been reported. Interoperability issues have also been faced calling for the use of standardized interfaces.

A number of information security threats have been identified, and will be further analysed in a complete risk analysis to prioritise risks and possible measures.

The use cases tested so far are focusing on data collection. Next steps will be to test use cases with which utilises collected data for smarter planning and operation of the distribution system.

REFERENCES

[1] Advanced metering and control systems. – Summary of public enquiry and final regulations.
NVE Document no. 7 2011

[2] I. A. Tøndel, M. G. Jaatun, M. B. Line
Security Threats in Demo Steinkjer
SINTEF ICT and Telenor Report
2012-09-12

[3] A. Shostack, "Experiences Threat Modeling at Microsoft," presented at the Modeling Security Workshop, Toulouse, 2008.

[4] M. G. Jaatun and I. A. Tøndel, "Covering Your Assets in Software Engineering," presented at the Second International Workshop on Secure Software Engineering (SecSE - ARES 2008), Barcelona, Catalonia, 2008.

[5] B. Schneier, "Attack Trees - Modeling security threats," Dr. Dobb's Journal, 2001.