NTNU
Norwegian University of
Science and Technology

D 4.1.1 Analysis of IoT Ecosystem

Konstantin Lenchik

Department of Computer Science and Media Technology
NTNU in Gjøvik
PO box 191
NO-2802 Gjøvik, Norway

Revision history

Version #	Description of change
0.1	Draft version 1 of report containing: introduction to Norwegian legacy energy grid and smart grid concept, Table of contents
0.1.1	Included more information about smart meter operation as suggested by supervisor
0.2	Draft version 2 of report with detailed analysis of production, transmission and distribution companies
0.2.1	Overview of stakeholders representing legislative, consultancy and software development domains
0.3	The graph of relations between stakeholders is added
0.4	Final version of report

Abstract

The paper under review presents the research of IoT Sec Ecosystem. The core of the ecosystem are production, transmission and distribution companies working together to deliver electricity to consumers and prosumers. One of the recent challenges is requirement to implement smart meter and required infrastructure. Paper investigates stakeholders that get involved in order to make the smart meter infrastructure reliable and secure. Among those are: consultancy, security and software companies; legislative and research actors. For each group of stakeholders, few reference companies are analyzed in detail

Current research was carried out in order to contribute to establishment of Smart Grid Security Center (SGSC) - independent research organization aiming to accomplish and promote best practices in field of Smart Grids Security. To better understand functions of SGSC, the graph of interconnections was developed. Nodes include stakeholders and SGSC, while edges represent relations, e.g. functional communications. Communications are both mono and bi-directional; thickness of edges also vary based on frequency of communication. From the graph it is seen, that SGSC should not aim to become an industry-specific consultancy organization, rather a scientific "umbrella" for all research and industrial activities carried out in the field

Contents

1 Introduction

1.1 IOT concept

The Internet of Things is a concept of environment where everyday devices possess identifying, processing and networking abilities, so that they are capable to interact with each other over the Internet. Moreover such devices are expected to be contex-aware, intelligent and ubiquitous. Similarly to any information system, IoT will consist of hardware, software and architecture. Hardware is a core component in such devices aiming to gather input data and often do a preliminary processing of it (for example fire alarm). Hardware can include RFID, NFC and other sensors. Even though many devices are capable of acting solely on hardware, in order to achieve interoperability, mature software (including middleware) should be developed [1].

1.2 Smart grids and their components

1.2.1 Legacy power grids

The classical electrical network aims to deliver electricity from suppliers to customers. Network consist of an utility producing electricity, high voltage transmission lines that carry power from distant sources to demand centers, and distribution lines that connect individual customers. In other words, grid consists of Production, Transmission, Distribution and Consumption parts (Figure 1).

Power stations may be located near a fuel source, at a dam site, or near renewable energy sources, and are often located away from heavily populated areas. The electric power which is generated is stepped up to a higher voltage at which it connects to the electric power transmission network. The bulk power transmission network will move the power through long distances, sometimes across international boundaries, until it reaches its wholesale customer (usually the company that owns the local electric power distribution network). On arrival at a substation, the power will be stepped down from a transmission level voltage to a distribution level voltage. As it exits the substation, it enters the distribution wiring. Finally, upon arrival at the service location, the power is stepped down again from the distribution voltage to the required service voltage(s).

Disadvantages of traditional grids:

- **Old system layout –** If the electricity is to be transmitted through long distances, losses are big. Moreover, more substations are needed to ensure proper delivery

- **Accounting and Billing –** In traditional infrastructure data collected from the meters is highly distributed, hence can not be aggregated for centralized analysis. It makes impossible having diverse costs of electricity consumption (e.g. cheaper during some hours, more expensive during others).

- **Difficult to plan production**- On the production site it is impossible to make a precise planning due to inaccurate and not timely data from customers

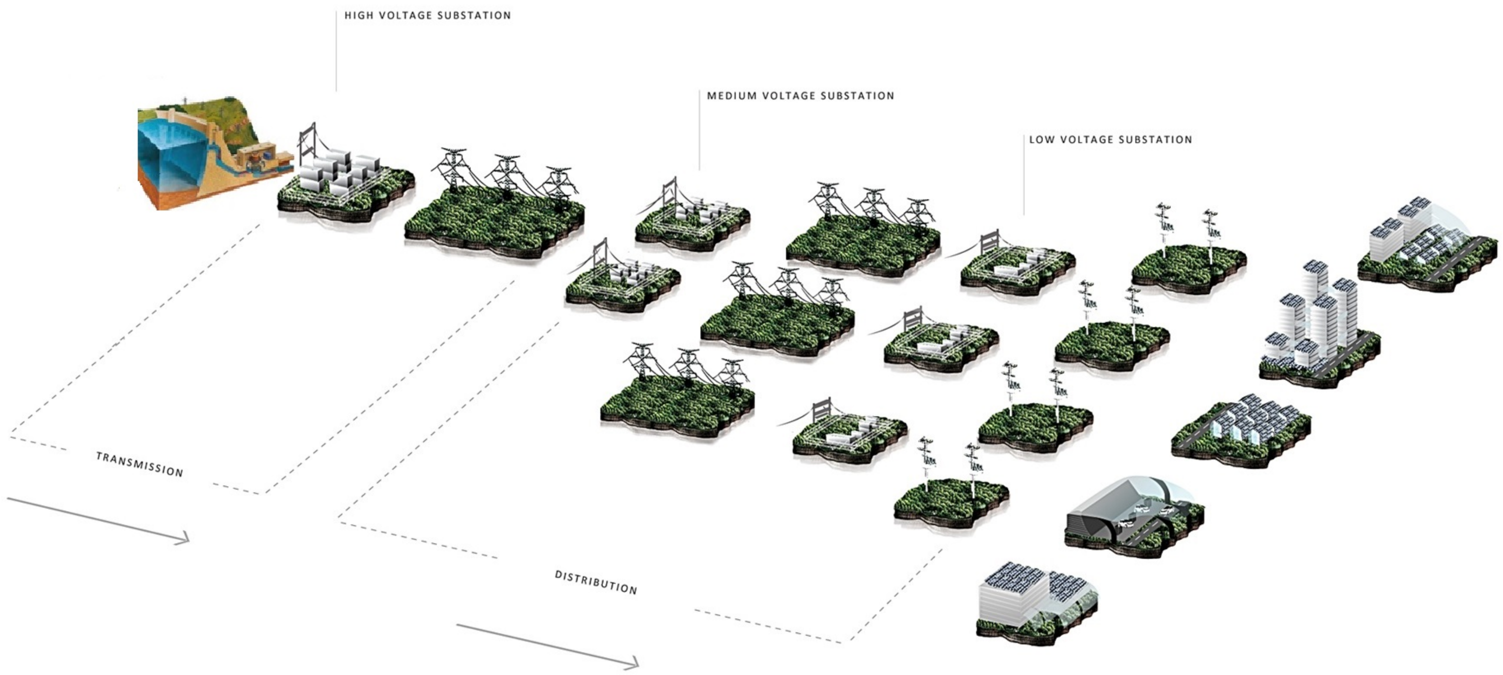


Figure 1: Structure of traditional electricity network.

- **Aging infrastructure –** The traditional power grid has been on the market quite for a while. As equipment gets older, it suffers from more failures and requires higher maintenance costs. More important that modern customers want to have failure rate above 99.5%, however it is infeasible to achieve with such an infrastructure [2]

1.2.2 Modern smart grids

On contrast to traditional power grid, smart grids are aiming to eliminate existing disadvantages. Smart grids use so-called state-estimation approach, which helps to eliminate failures and allow self-healing, without actual involvement of technical personnel. The network topology of the grid is more flexible, allowing bidirectional energy flows and distributed generation of electricity. Flexibility means that more customers or prosumers can be connected to the grid without altering its structure too much. Distributed production results in lower losses during transmission, as transmission distance decreases.

As Grid becomes more fault-tolerant, it has less need for redundancy. This is achieved by making energy supply adjustable to the current grid load, i.e. turn off powerful electrical devices during sudden peaks in energy consumptions. If such peaks will be smoothed, energy producers will not need to maintain redundant power plants.

Another focus of smart grids is on renewable power generation. Connection of such utilities into a smart grid will strategically manage the diverse and geographically scattered renewable power sources like wind farms, solar plants, and hydro stations. Smart grid will ensure that this energy can be stored safely and distributed where and when it's needed.

Moreover, smart grids in a broad sense comprise not only electrical energy value chain, but also neighbor domains such as smart vehicles and smart homes on Figure 2.

Smart home concept means basically that home systems and appliances are connected to internet, available to share data and provide remote management. For example, HVAC (heat, ventilation, air conditioning), lighting systems can all be automated and manipulated by remote control. Various electrical appliances such as washing machines, dishwashers, refrigerators, and cooking devices can be programmed to carry out their tasks. Radios and TV sets, as well as other entertainment devices, can be connected to share programming channels.[] A lot of effort is put in trying to make devices not only being remotely manageable, but observing habits of the inhabitants, make some aggregation and make decisions (i.e. adjust power) based on historical information available.

Another prospective area is creation of elderly people monitoring system, while they are at home. The idea is to reduce cost from keeping elderly people requiring health monitoring in designated hospitals, while allowing them to live at home with a system monitoring their health and reporting critical changes to the specially trained service desk. Several European projects, like ENABLE, HIS, SmartBo, TERVA and PROSAFE have made considerable advances in this area. []

1.3 Security, Privacy, and Dependability

In the smart grid domain, information security is usually viewed as part of Security, Privacy, and Dependability (SPD) analysis. Security focus is mainly on home control unit and control center. Malicious intervention to first one might result in troubles for a single household, while disruption of control center operation can result in problems for all

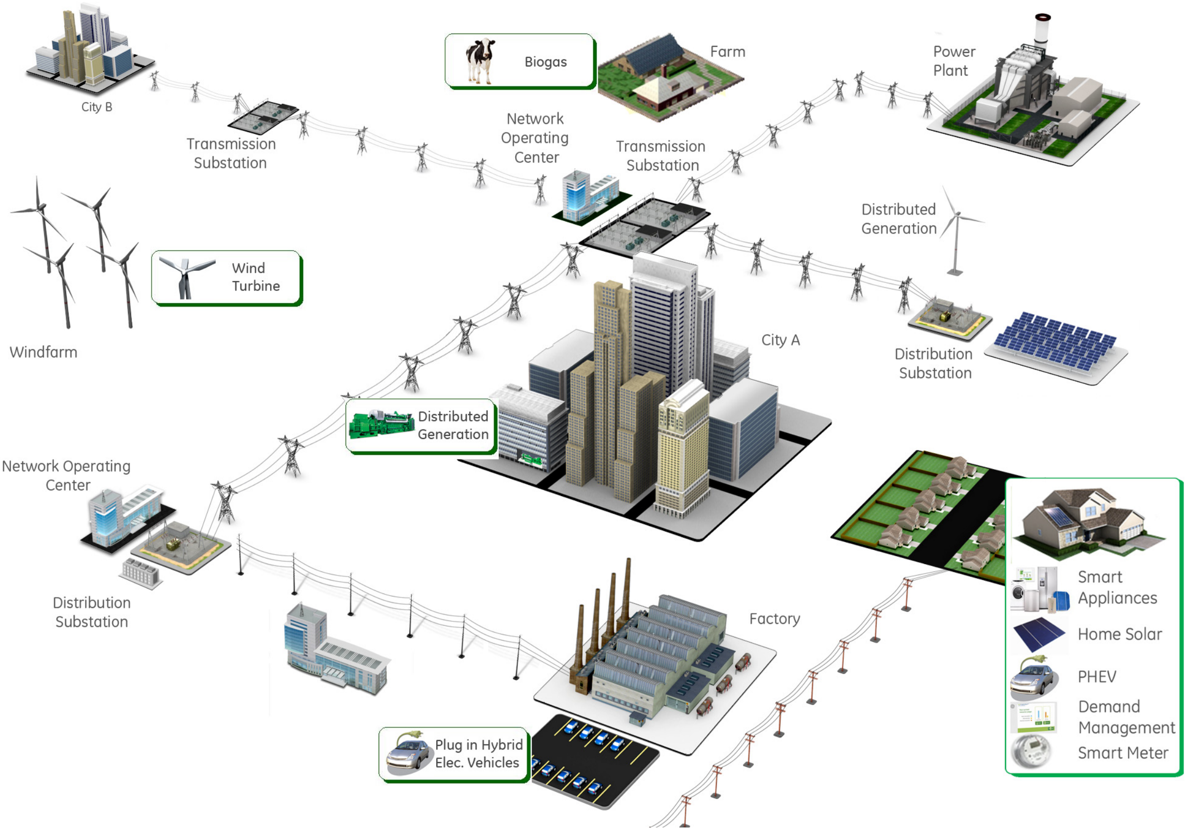


Figure 2: Core components of smart grids.

households in the area of operation center responsibility. Main focus of Privacy is on data allowing to monitor habits of residents. Violation of privacy can begin from crock getting data during one of the following stages: transfer, conversion, formatting or storage. If it was possible to make some conclusions from aggregated raw data, those conclusions can be distributed further for malicious intents. For example: blackmailing of residents, planning a burglary or illegal marketing purposes. Dependability concern is on supplying electricity without interruptions and achieve Grid stability of at lest 99,96%. [3]

One of the goals of this project is to define Smart Grid Security Center, that will promote secure smart grids for all parties involved. Through the project I will analyze interconnections between existing members of smart grids ecosystem and offer proper place for SGSC on the graph. The challenge for positioning SGSC is to achieve primary goal, e.g. promote security, while do not disturbing existing collaboration interfaces or entering into "competition" with other regulative or advisory institution.

2 Smart Grids Actors

2.1 Defining groups of actors

To narrow down the scope of this work, we will focus on Smart Meter value chain. It‘s primary stakeholders are companies involved in: Production, Transmission and Distribution of energy. However there are other actors tightly interacting with those. Below is the preliminary categorization of actors in IoTSec Ecosystem:

1. **Production of energy**- Power utilities, producing traditional and renewable electrical energy.

2. **Transmission System Operators (TSO)** - In Norway only Statnet can be classified as a member of this group by definition. However according to alternative definition, owners of regional electrical network can be also considered as TSOs.

3. **Distribution System Operators (DSO)**- responsible for operation of local electrical grid between TSO and customers or prosumers.

4. **Security companies** – carrying out projects and developing solutions for security of smart grids. This includes security of individual households and grid operators.

5. **Software development** - companies providing different software and middle ware solutions. To limit the scope of the paper, we will focus only on software related to Smart Meter value chain.

6. **Manufacturers of smart energy service devices** - vendors providing smart meters, communication system modules, etc.

7. **Consulting**- companies providing advisory and consulting services for energy companies. Having best practices in place and list of reliable suppliers they take active participation in the projects launched by power companies.

8. **Legislative**- This group unites governmental companies, capable of creating new laws in power industry as well as companies working on promoting rights of their stakeholders in focus (trade unions and company unions).

9. **Research**- Research institutions take active part in various energy projects.

10. **Prosumers and Customers**- Customers and prosumers are end-users in electricity market. Naturally actors influencing this value chain should be also analyzed. [4]

In the following sections I am going to discuss members of each group in detail.

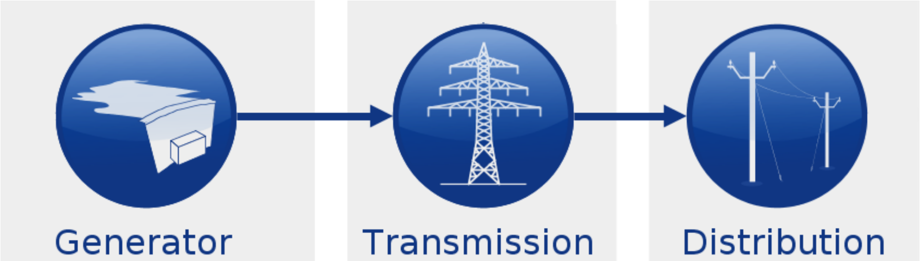
2.2 Production of energy, TSO, DSO

2.2.1 General structure of stakeholders

The main companies involved in electricity production and delivery to customer are power generation, transmission and distribution companies. In Norway ca. 98% of electricity is hydro-generated. Other means of generation includes solar power and wind power and couple of plants burning natural gas. Norway has built 4 nuclear reactors, but they are not used for power generation, rather for research purposes. [5]

There are quite a number of companies, that can be associated with single or multiple groups, so below on Figure 3 I provide high-level classification.

1. Production of energy
2. TSO
3. DSO



Governmental companies, being owners of many other companies:

Statkraft	Statnett

Companies acting alone in all 3 sectors:

Haufslund
Eidsiva
ISE
Helgeland Kraft
Istad
Lofotkraft
Lyse Energi
NTE
Nordmøre Energiverk
Sognekraft
Svorka Energi
Troms Kraft
TrønderEnergi
Varanger Kraft

Companies who are acting in two sectors:

BKK	Fjordkraft
Agder Energi	LOS (daughter of Agder Energi)
Nordkraft	
Skagerak Energi	
Tinfos	
BE Produksjon AS (Bodo Energi)	BE Kraftsalg AS
Salten Kraftsamband	Salten Kraftsamband
Glitre Energi	Glitre Energi

Companies working in one sector only:

E-CO Energi
Arendals Fossekompani
Firma Albert Collett
Akershus Energi
Industrikraft Midt-Norge
Kraftverkene i Øvre Namsen
Naturkraft
Norsk Hydro
Østfold Energi

Nordlandsnett
Energi Nett AS

Askøy Energi (d: FEN)
Røyken Kraft (d: FEN)
Follo Energi (d: FEN)
Norgesnett Fredrikstad

Figure 3: Production of energy, TSO and DSO.

2.3 Distribution of energy

2.3.1 Glitre Energi

The company operates in Akerhus (Buskerud region) and Oppland (Hadeland region) counties. Glitre energy is a concern comprising areas of business activities in electricity production (Glitre Energi Produksjon AS), Distribution (Glitre Energi Nett AS), Electricity Supply (Glitre Energi Strøm) and supplementary electricity related activities (optical cabling, central heating, etc.). Production of electricity incorporates control of 20 hydroelectricity plants, where 13 are owned completely and 7 are owned partially.

Glitre Energi Nett is a distribution operator for over 170 000 habitants in Nedre Buskerud and Hadeland. In order to keep customers satisfied they regularly invest into development of long-term solutions in the areas of environment protection and uninterrupted energy delivery. The concern is indirectly owned by Buskerud commune.

Regulative authorities

Glitre energy, gets most of it regulations from the NVE. Beside that concern actively cooperates with Energi Norge and Rasjonell Elektrisk Nettvirksomhet. The last provides different “frame” advices regarding increasing efficiency and quality of primary business functions (delivery of electricity). Glitre Energi is not a part of Nettaliansen.

When it comes to research activities they actively cooperate with Smart Grid center (Trondheim), however the research area does not include information security questions.

Information security approach

In general information security issues are expected to be handled by internal department. However, if the case got escalated there are number of subcontractors (partners) that can be involved. Any software- related security is expected to be handled via service-level agreement. This implies that software vendors or those who do actual installation are responsible if any security issue will happen during operation. Main concern- is secure data exchange between nodes in smart meter chain.

Incident handling practice does not possess robust policies, hence company is looking for more consultancy help in this area. Glitre Energi is part of KraftCERT, with the benefit of getting regular warnings and recommendations regarding acute treats in energy sector. However KraftCERT does not have the obligation to do actual incident handling, so company in future would like to invest into their own Emergency team for Incident Handling and Disaster Recovery.

Preservation of customer‘s data Privacy is not an acute question right now, however, the situation is expected to change after new regulations from NVE will be pushed in late 2017. The current state of affairs is that they get general requirements from Datatilsynet and try to implement them with some consultancy help. Any input from SGSC will be welcome.

2.3.2 Fredrikstad Energi (FEN)

The company is organized in a concern, performing activities in areas like Distribution (company Norgesnett), Supply (Follo Energi, Askøy Energi, Fredrikstad Energi) and others. FEN has roughly 88 000 customers in county of Ostfold. [6]

FEN owns and leads a research program Smart Energi Hvaler. In an island commune of Hvaler (Ostfold county) the research project is established to perform different activities in local energy sector in the domain of smart energy. Essentially active support is provided from NCE Smart. [7]

Regulative authorities

Having NVE as a main regulative authority, company also cooperates actively with Rasjonell Elektrisk Nettvirksomhet (REN) to get industrial best practices . On the other hand, FEN actively cooperates with Smart Grids Center (Trondheim) in area of research and unfolding of smart grid networks.

Information security approach

The company relies on own information security department, however has assumptions that not all the essential information security functions can be performed on their own. Some of the security risks are transferred by service-level agreement with Software vendors (this is primarily in the field of SCADA security). Company prefers to view security from the legal perspective first, meaning once they get new security regulations from NVE, they first employ law help to better understand required scope of action and after go for actual technological implementation.

FEN seeks expert advice and industrial competence in the problem of privacy preservation of customer data. Especially when new regulations from NVE will come in to place. SGSC is concerned as a preferred partner for this problem. [8]

2.4 Security companies

There are various security companies involved in Smart Grids market. The solutions they provide are in the area of grid operators security or security of individual households. Even though grid operators mostly have own information security departments, they cooperate with security companies on certain matters.

2.4.1 KraftCERT

KraftCERT- is Computer Emergency Response Team for energy sector, created by Statnett, Statkraft and Hafslund. Similarly to CERTs in other industries, the main task of KraftCERT is to provide support for energy companies. This includes advices regarding IT systems in operation and Incident Handling. Having Incident Handling service as primary goal, KraftCERT performs following activities:

- Regularly accumulates (from members and external organizations) and analyzes data regarding incidents in energy sector. Consequently they issue advises for their members regarding vulnerability removal.

- Processes any data, that might help to avoid possible incidents or help discover new threats. Each threat is assessed according to severity level. Than members of KraftCERT receive information on recommended defense actions.

- Actively assists when member of power sector has incident ongoing. By default KraftCERT will provide active advices, incident handling plan, logging and analysis procedures, etc. If the additional agreement was signed, they can intervene and perform actual incident handling

- For the purpose of education, they organize seminars devoted to Incident Handling and can conduct a training activity, where company faces demo-incident [9]

Regulative authorities

KraftCERT actively exchanges information and follows guidelines from NorCERT, which is a department of National Security Authority (NSM). NSM in it‘s turn is a daughter authority of Royal Norwegian Ministry of Defence. At the same time they have a well-established cooperation with international CERTs.

2.4.2 Security control mechanisms for homes

EyeSaaS provides a cloud based service for remote configuration of customers equipment and perform diagnosis on connectivity at the customers home. In scope of smart grid market, the company provides security control mechanisms for homes.

2.4.3 Security companies offering services for Smart Grids

Mnemonic is one of the largest providers of Information Security services in Nordic countries. The company consists of over 120 security professionals and has offices in Oslo, Stockholm, Stavanger. Mnemonic was among companies who founded KraftCERT. Company provides robust security services including threat research, advanced targeted attack detection, incident response and ethical hacking services.

Mnemonic has large client base among DSOs. The information regarding particular security services offered to clients is not publicly available, however current target of Mnemonic is to supply DSOs with a robust network sensor integrated into IDS/IPS systems. [10]

Regulative authorities

Mnemonic primary contacts NVE in regard of regulations. They have contacts (consultations) several times a year.

NetSecurity is a daughter company of Agder Energi specializing on security of corporate network. Typical services are:

- Protection of corporate network, including unfolding of Firewall, Penetration testing, End point security.
- Security analysis and unified security managements.
- Incident response.

Regulative authorities

Main regulations come from NVE and NEK. No cooperation with Smart Grid Center Trondheim is expected in nearest future.

2.5 Software development

There are quite many IT systems functioning on different stages of Smart Meter value chain. For purpose of this paper I will limit overview to the IT solutions, that are situated between consumers, DSOs and power suppliers.

2.5.1 Map of IT systems between consumer and DSO

IT systems can be classified on high level, as those operating on Meter Point, DSO, Power supplier. On Picture 4 below I present overall map of IT systems allocation.

Meter point consists of Head End System and Meter Data Management System (MDMS). The Head End System is provided by **Valider**, Ominia solution by **Kamstrup** and **Safe Base** while MDMS is delivered by ESmart systems.

Operations at the point of DSO can be presented as a 4 part kernel with allied systems. Each part of kernel is responsible for operations in: Data Hub, Smart Meter, Utility and Smart Grid. Those 4 parts nicely reflect core functionality of DSO. **Greenbird** company provides Metercloud solution, performing operations on each part of kernel. As example of allied systems, we can take ADMS system by **ABB**.

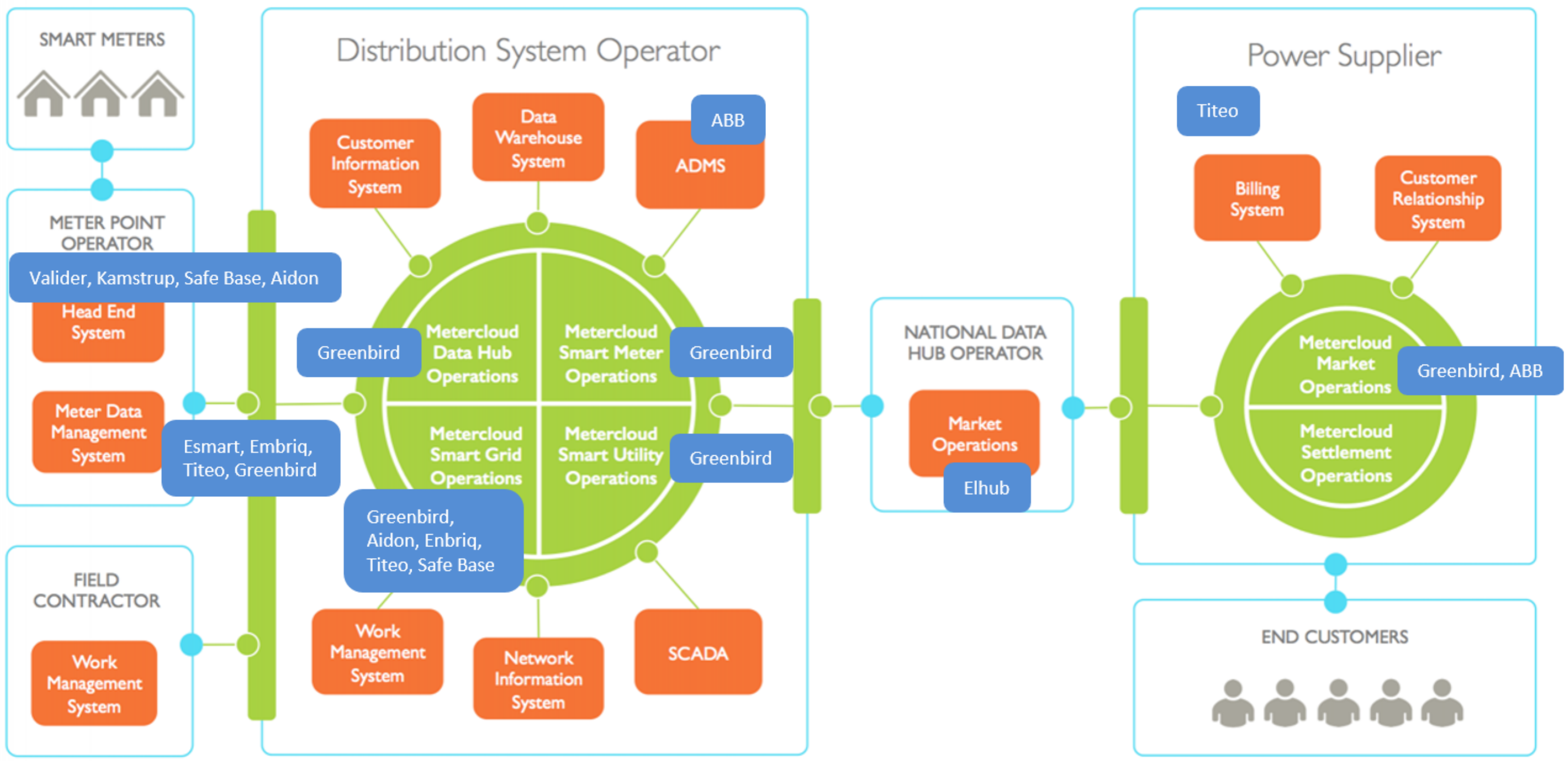

SMART METERS
METER POINT OPERATOR
Valider, Kamstrup, Safe Base, Aidon
Head End System
Meter Data Management System
Esmart, Embriq, Titeo, Greenbird
FIELD CONTRACTOR
Work Management System
Distribution System Operator
Customer Information System
Data Warehouse System
ABB
ADMS
Greenbird
Metercloud Data Hub Operations
Metercloud Smart Meter Operations
Greenbird
Metercloud Smart Grid Operations
Metercloud Smart Utility Operations
Greenbird
Greenbird, Aidon, Enbriq, Titeo, Safe Base
Work Management System
Network Information System
SCADA
NATIONAL DATA HUB OPERATOR
Market Operations
Elhub
Power Supplier
Titeo
Billing System
Customer Relationship System
Metercloud Market Operations
Greenbird, ABB
Metercloud Settlement Operations
END CUSTOMERS

Figure 4: Structure of Information systems.

According to the new regulations, consumer data (e.g. consumption and price per unit) should be stored at National Data Hub Operator. **Elhub**, which is going to be launched soon will take up this role. Last actor in this chain is Power supplier. They have two main IT systems: Market operations and Settlement operations. **Greenbird** supplies both systems. **ABB** provides ABB Network Manager MMS for market operations. Billing system is provided by **Titeo**.

2.5.2 Safe Base

During the project it was possible to briefly analyze **Safe Base** - a company with vast telecommunication background, providing two solutions for Smart Grids market: Head-end system at Meter point and SafeMon- Monitoring system at DSO‘s Smart Grid operation site. The last is supposed to use artificial intelligence to actually predict failures on low voltage power lines. Combined with possibilities to determine actual point of failure on the line, the product looks promising, and according to developers can increase life expectancy of grid up to 10 years.

Regulative authorities

The company have almost none interaction with NVE, while actively interacts with REN retrieving guidelines for smart alarm installation and data retrieving. Safe base is a member of Smart Grids Center Trondheim and benefits from it by getting better insight of the Smart Grids industry.

2.5.3 Greenbird

The Greenbird company was analyzed in detail. Greenbird delivers Metercloud, which is system integration delivered as an enterprise SaaS. Metercloud has out-of-the-box support for all common business processes for operating smart metering and smart grids. It is an alternative to running custom integration projects based on traditional middleware from incumbent vendors like Oracle, Microsoft or IBM. Being SaaS, Greenbird is building a full ecosystem for application vendors supporting operation of smart metering and smart grids. System integration is a huge barrier for software vendors offering solutions like e.g. MDM and DMS. Once application developers enter into partnership agreements with Greenbird, they get Metercloud connectors for their applications. This secures that DSO can onboard new solutions within days with configuration instead of several months with custom development of integrations. [11]

Customers

As it seen from the map of IT systems structure (Picture 4), currently main customers for Metercloud solution are DSOs. However they received Series A funding of 5 million USD in November 2016 to develop Metercloud and expand internationally. In future company aims to take a substantial global market share for system integration for utilities. Another possible vector of development is to extend the support to include integration with systems for production planning and transmission. In this direction company already has demo products to handle data from substations.

2.5.4 Other systems

In order to give example from another domain, I will do short review of Smart Energy suite by **Powel**. This software suite can be used by power companies of different size. The core goal is to provide a reliable tool for production planning both long term and short term. As an input, Smart Energy uses powerful forecasting mechanisms and trading data. As an output it provides optimized production plan.

Powel is focused on hydro energy, as it is dominated on Norwegian market, however developers clamed that it is applicable to other means of power generation. On Picture 5 below the functional structure of Smart Energy suite is presented. Starting from the left, input data and forecasts are collected and verified. The long term strategy is normally represented as a water value or end-level window per reservoir, calculated once or twice per week by seasonal planning tools.

Once all input data is gathered, software offers optimal bids for the next day trading market (Elspot). Next it receives obligations (contracts) from counter parties that are to be fulfilled and naturally optimizes production plan. Last stage is interaction with TSO. Next day, during actual operation, software monitors production progress, to know actual outrages, as well as monitors daily secondary market (Elbas). Based on those inputs, software makes required alternations of production plan.

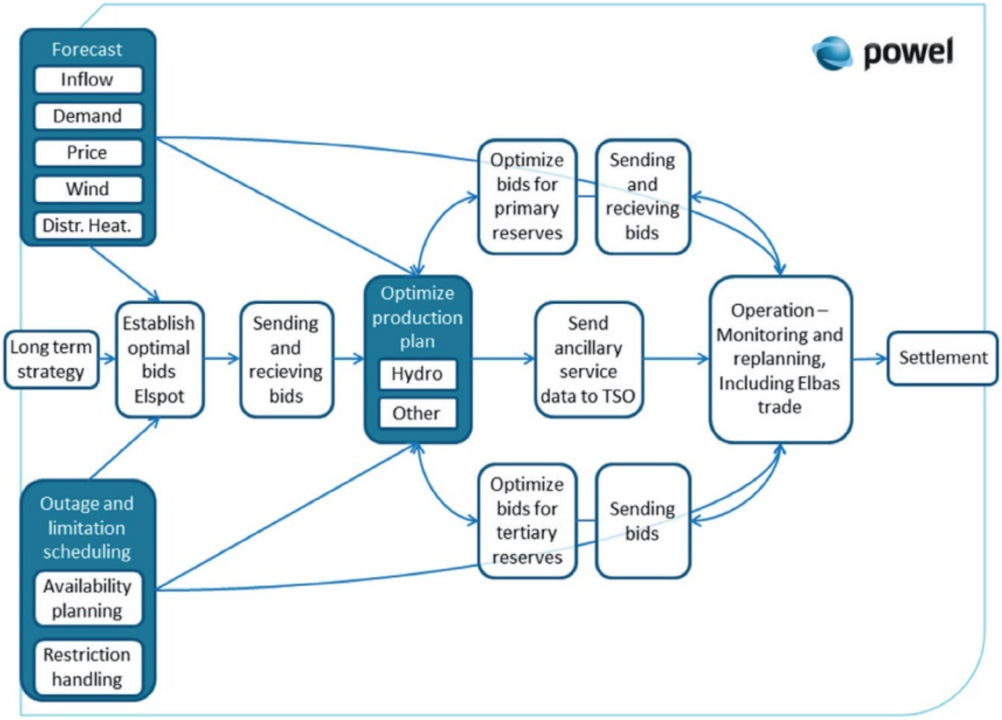

powel
Forecast
Inflow
Demand
Price
Wind
Distr. Heat.
Long term strategy
Establish optimal bids Elspot
Sending and recieving bids
Optimize production plan
Hydro
Other
Optimize bids for primary reserves
Sending and recieving bids
Send ancillary service data to TSO
Operation – Monitoring and replanning, Including Elbas trade
Settlement
Optimize bids for tertiary reserves
Sending bids
Outage and limitation scheduling
Availability planning
Restriction handling

Figure 5: Smart Energy suite by Powel to adjust production plan.

2.5.5 Raw structure of companies in SW domain

As some of companies are acting in overlapping domains, below I provide a list structure of companies from Software domain:

1. Meter point Operator

    1.1. Head end System

        1.1.1. Kamstrup

1.1.1.1. OMNIA solution

1.1.2. Aidon

1.1.3. Valider

1.1.4. Safe Base

1.2. Meter Data Management System

1.2.1. Greenbird

1.2.1.1. Metercloud solution for DMS

1.2.2. Embriq

1.2.3. Titeo

1.2.4. Esmart

2. DSO

2.1. Smart grid operations

2.2. Greenbird

2.3. Aidon

2.3.1. Embriq

2.4. Titeo

2.5. Smart meter operations

2.5.1. Greenbird

2.6. Smart utility operations

2.6.1. Greenbird

2.7. Data Hub operations

2.7.1. Greenbird

2.8. ADMS

2.8.1. ABB

2.8.1.1. Network Manager ADMS

3. Power Supplier

3.1. Billing systems

3.1.1. Titeo

3.2. Market Operations

3.2.1. ABB

3.2.1.1. ABB Network Manager MMS

3.2.2. Greenbird

4. Automatical planning for Power production companies

4.1. Powel

2.6 Consulting

Consulting companies specialize on providing expert advices not only to companies but also individuals for a fee. In this chapter I review 3 consultancy companies, acting on a Smart Grids market.

2.6.1 Power industry consulting

Epos consulting is an energy niche consultancy company consisting of 4 top experts in energy (Magnar Bjørk, Fredrik Bjørk, Tom Wirkola, Rune Pedersen). Company has broad experience for working in Utilities, for ICT-solution suppliers and consultants; hence they have developed a «niche area where ICT meets electrical engineering». They specialize in designing, developing and managing Smart Grid related projects for Norwegian utilities. Specifically providing consulting services, related to analysis, strategy, project design and development, applications for funding of R&D / Demo-projects and project management.

Customers and Suppliers

The company provides services to Power generation, TSO and DSO. However most customers are DSOs. Among key customers there are Hafslund ASA / Hafslund Nett, Statnett, Glitre Energi, Ringeriks-Kraft.

As any consultancy company, they need to cooperate with suppliers. The company focuses on being neutral in terms of working with suppliers of solutions so far, but have a broad contact network with solution providers in the Norwegian Market. [12]

Regulative authorities

The primary regulatory / legislative influencing their work is NVE. As their customers are energy customers, Energi Norge, the company union of energy companies, can be defined as secondary authority. Epos Consulting is not a member of industry specific company union, as there are no union or industry association for energy related consultant companies.

Future plans

Epos consulting in future does not plan to severely change their specialization or explore new markets. They have intention to concentrate on their niche and be solutions architects, projects developers and project managers. If along this way they find solutions / partners to work together with they would certainly be interested in such to further develop the business.

2.6.2 Heating efficiency consultancy

Norsk Enøk og Energi (NEE) is a medium size consultancy company with 26 employees in 4 offices, possessed by Fredrikstad Energi. The company‘s areas of interest are energy consultancy and development of energy projects. Special focus is on renewable heat production and increase of efficiency of energy solutions.

Many projects carried out are related to Energy Performance contracting, where NEE suggests and analyzes possible ways to make efficient centralized or decentralized heating. They follow up the construction project from design to implementation stage and always consider possibility to apply renewable heating solutions.

2.6.3 Market operation consultancy

Markedskraft operates is large-size (more than 500 clients in more than 30 European countries) consultancy company focusing on energy market research. They provide services like assisting throughout the entire value chain including fundamental market analysis, advisory services, risk management, financial portfolio management and physical handling and settlement.

Markedskraft have own product “MK online” allowing professionals to forecast long term and short term prices. They also do portfolio management on the wholesale power market.

2.7 Legislative

2.7.1 Government

The main governmental companies, supervising the economy sector are *Norwegian Water Resources and Energy Directorate (NVE)* and *Norsk Elektrisk komite (NEK)* . NEK is responsible for Development of standards for electrical devices and networks. NVE develops requirements related to information security for the DSOs and other actors on the market.

Information security requirements for DSOs

The last official regulation was published in September 2012[13]. Authors highlighted, that AMS security incident can have direct impact: disruption of electricity supply to consumer, in other words make it impossible to perform core business objective. Hence information security should be treated as highly important. The document is structured in a sections, among them were:

- Section A: General security requirements to DSOs
- Section B: Regular Risk analysis, with reaction: training and review
- Section C: Access control
- Section D: Incident Handling procedures

Consumer privacy protection

As an input for the requirements they analyze field expertise, provided by DSOs, as well as general information security requirements coming from Data Protection Authority *(Datatilsynet)* . The recent cooperation of NVE and Datatilsinet was aimed to protect the right for consumer privacy and to prevent misuse of personal data, in regard to Smart Grids domain. Privacy regulations were published as draft [14], but expected to be finalized by the end of 2017. The NVE department Beredskapsseksjonen will be responsible to issue, update and monitor compliance to the regulations. Previously department was dealing with questions of SCADA system security.

2.7.2 Company unions

The most powerful company unions in Norway are Energi Norge, KS Bedrift Energi and Nettaliansen. The role of company union implies consulting activities towards their members (DSOs). Below I provide overview of KS Bedrift Energi.

KS Bedrift Energi

KS Bedrift Energi is the department of the KS Bedrift operating in the energy sector. Scope of their activities include:

- To promote interest of their members
- Provide support regarding employer‘s issues of any kind
- Legal guidance

Company‘s Information security is ensured by own department, however security companies, are often hired as contractors.

Being a company union organization, they aim to keep their members updated (notify and train) with all relevant information. NVE is the main regulative authority, hence KS Bedrift regularly monitors regulations coming from them. In order to provide even greater help for the DSOs, regulations are analyzed and forwarded only with subsequent clarifications and explanations. Some supporting material comes in a form of leaflets, while other are communicated through specially organized trainings.

When it comes to the information security trainings, company does not expect to accumulate enough field expertise, hence security companies and SGSC are welcome to provide help.

KS Bedrift Energi cooperates with Smart Grid Center Trondheim only upon launch of pilot projects.

Sol Energi Klyngen

The cluster was established in 2013 with a goal to strengthen the Norwegian partners' innovation capacity and competitiveness and to take a bigger share of the global energy market. Having united energy companies, R&D organizations and educational institutions, they aim to strengthen interaction and cooperation on the market.

Market areas of the cluster are:

- Sustainable production of materials.
- Building-integrated solutions.
- Micro-distribution.
- Energy systems.
- Energy services.

Sol Energi Klyngen currently cooperates with NCE Smart and Smart Grid Center regarding smart grid projects, however plans to enhance their partner network in the future.

Smart Grid Center Trondheim

Smart Grid center was created as a result of recommendation from Olje- og energidepartementet (OED). The center (organized as a membership organization) has an aim to be a main coordinator of the research activities in the area of Smart Grids. A lot of research activity is carried out from cooperation of SINTEF and NTNU, however center has a wide range of industrial partners. Among goals of the center are:

- Develop demo sites for research and testing of smart grid projects.
- Exchange knowledge and promote robust solutions for AMS.
- Micro-distribution.
- Focus on standardization and interoperability of smart grid solutions.
- Promote activities within security and reliability of Smart Grids.

Due to excessive deployment of AMS and general research interest in Smart Grids, center does not have yet conducted any serious activity in the field of IT Security.

2.7.3 Customer support organization

Forbrukerrådet

Forbrukerrådet is an independent interest organization supporting consumers. The organization work with both consumers and service providers. Consumers can get general advices regarding consumer-provider relations, while providers receive education on consumer-friendly approach . Forbrukerrådet would like to provide their comments and recommendations towards upcoming services related to IoT and Smart Grids

The Department of digital service will work on advising consumers, who get Smart Meter installed. Specifically they would like to have a set of guidelines for the consumers, containing advices on:

- Privacy protection
- Right for uninterrupted power supply

[15] To achieve goals above, they would like to engage field experts, possibly SGSC to develop necessary guidelines. The company does not expect themselves to become experts in field of information security.

2.7.4 Private organizations

Rasjonell Elektrisk Nettvirksomhet AS (REN AS)

Private organization REN has an aim to develope and promote recommendations (sometimes standards) for energy companies aiming to increase efficiency of operation and quality of services. Even though company has only 14 employees, it is owned by 61 DSO and have more than 120 DSOs as customers. Members of the board are management of energy companies like Hafslund Nett AS, Lyse Elnett AS, BKK Nett AS, etc. as well as trade unions Energi Norge. The main areas of competence are:

- Projecting.
- Installation.
- Maintenance.

Key findings are distributed between members with help of RENblader. The company has a goal to regularly update their members with industry best practices and conduct external and internal courses. REN also offers range of web tools to increase knowledge value of their customers.

However, being an important actor on the market, REN does not issue any standards recommendations related to IT security.

2.8 Research

Research domain contains higher institutions (UiO, UiS, NTNU, UiT, etc.), private(SINTEF, Trøndelag Forskning og Utvikling, etc.) and governmental research organizations. Common characteristic is their goal to foster introduction of Smart Grids in Norway. Below I will present in detail Smart Grid Center Trondheim- one of the main actors on the arena of smart grids.

2.8.1 Smart Grid Center Trondheim

Smart Grid Center Trondheim (SGCT) was established in 2013 according to the suggestion from Oil and Energy department (OED). One of the challenges center aims to solve-is to fulfill European Renewables directive [16] : to achieve 67 percent of energy use is renewable energy. Even though today 98 percent of electricity generation is hydro-generated, there are many domains where non-renewable energy prevails, for example personal car usage.

The center is organized as a membership organization, and has following goals:

- Develop a clear guideline, how Norway can move towards Smart Grids
- Contribute to standardization and interoperability of smart grid solutions
- Provide labs (demo sites) for smart grid stakeholders to test their solutions

[17]

As for year 2017, SGCT does not have capacity to conduct research on information security of AMS value chain. However that action is in their backlog.

3 Graph of interconnections between stakeholders

3.1 High level picture of stakeholders

Current research was performed with aim to contribute to establishment of Smart Grid Security Center (SGSC) - independent research organization aiming to accomplish and promote best practices in field of Smart Grids Security. From the analysis of actors performed above, some gap between intended information security and actual information security can be detected. SGSC can be called to close this gap.

Consider a simple graph on Picture 6 below. Beginning from the right side of the graph, regulations are coming from NVE, who in their turn receive some input from Datatilsynet, and from REN. Destination of those regulations are DSOs, who are obliged to comply to regulations. Actual regulations are denoted with blue arrow, while prospective regulations are presented with yellow arrows. In regard to scope of this research, I selected 5 most important requirements from regulative authorities to the DSOs (pictured in the left most column):

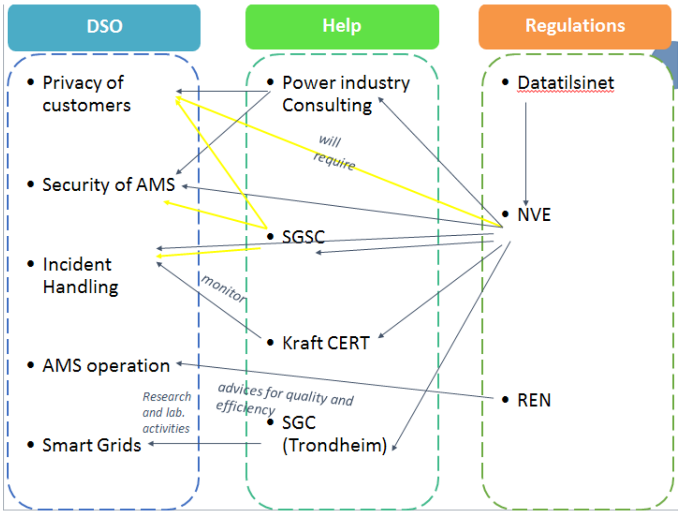


Figure 6: High level graph of stakeholders in AMS value chain.

- **Privacy of consumers**- procedures and technology to ensure, that privacy of people on the consumer side is not compromised. While data containing electricity consumption is not confidential, it has to be protected from being publically available. Possible threats are bulglary, black marketing, etc.
- **AMS operation**- Ensure proper operation of AMS, installation and maintenance guidelines
- **Incident Handling**- Have a robust procedures related to incident handling; Posses a team or have an agreement with supplier to intervene if the actual incident is ongoing. Monitor relative incidents in energy sector, apply defense actions.

- **Security of AMS**- Ensure that AMS are secure, can not be penetrated or manipulated
- **Smart Grids**- move towards implementation of next stages of smart grid infrastructure.

Not all of this regulations DSOs are capable to fulfill on their own. Moreover, some regulations need fundamental subsequent research activities. Hence there are actors in between (pictured as Help, middle column). The Consultancy companies are capable to provide advices on preservation of customers privacy and AMS security. KraftCERT delivering the field expertise of Power sector incidents, will perform monitoring and advising roles. Specifically they will update members regarding threats, vulnerabilities and related incidents happened; Kraft CERT can also provide incident handling services. However none of above listed organizations can accumulate all information security consultancy functions, hence SGSC can contribute to all security-related issues.

3.2 Adding more granulation to Legislative domain

The high level graph presented above is a good starting point, however it is more complicated in reality. Consider the role of SGSC, as a research institution, that accumulates knowledge on information security related questions. As an input SGSC gets regulations from NVE and that output can be in a form of advice or in a form of actual implementation on the production site (denoted as Advisory and Consultancy on Picture 7). Due to prevailing research vector, the center does not expect to become a robust consultancy company, having those services as a core income source. Rather SGSC would like to transfer implementation stage of such projects to the security companies. However, security companies do not posses enough expertise so far in the field of Smart Grids. Hence they need cooperation with energy consultancy companies. As a result cooperation of SGSC, Security companies and consultancy companies can deliver precise and reliable service to the customers (DSOs).

One of the important actors are Company Unions and Customer Care organizations. Even though they do not perform strictly speaking legislative function, they issue recommendations for the DSOs. Naturally DSOs listen and follow recommendations, coming from companies who have main goal to provide DSOs care. None of the company union organizations have a goal to posses field expertise in information security, however they would like to be able to provide such information (in form of leaflets or trainings) to their member DSOs. Hence here is an opportunity for SGSC to cooperate with Company unions on the matter of providing navigation in information security requirements issued by Regulative authorities.

At the same time SGSC will also have direct communication with DSOs and provide advisory services directly to them. On Picture 7 this is denoted by blue, yellow and purple arrows going from SGSC to DSOs without intermediate stop in domain of Company unions.

3.3 SGSC as a marketplace

The graph discussed above provides good granulation on the structure of stakeholders, however still needs some improvement. After revisions, more detailed graph was suggested on Picture . Consider direction of information flow. According to the graph, it is mono

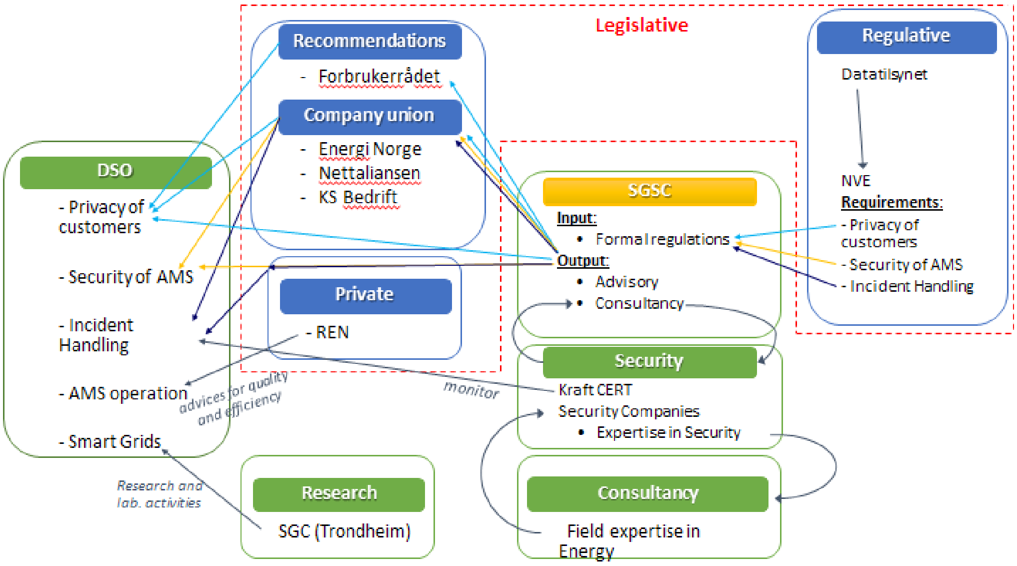


Figure 7: Detailed structure of Legislative domain.

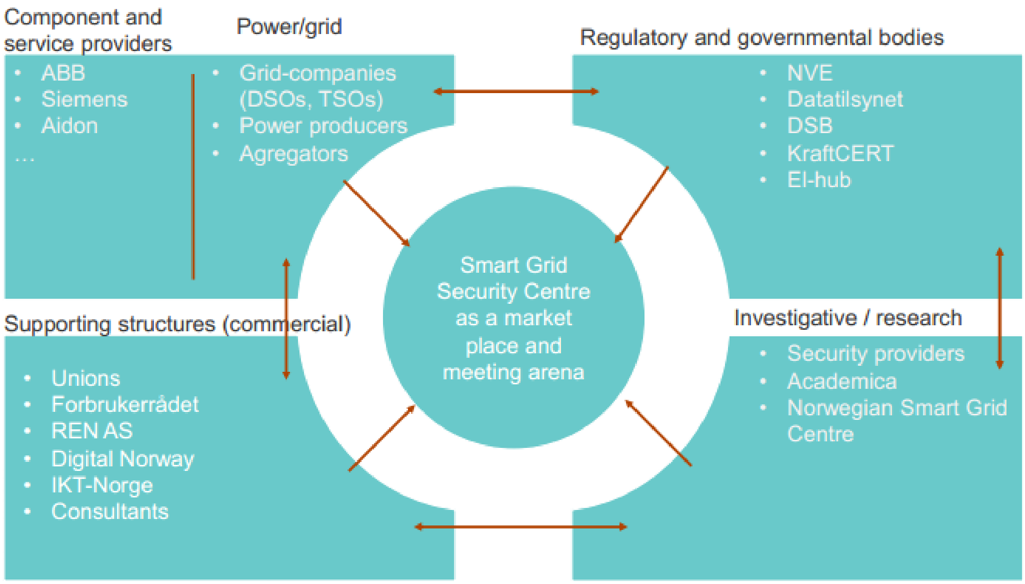


Figure 8: SGSC as a marketplace.

directional flow from NVE to DSO. This implies that NVE already possesses all knowledge of the domain. This is not completely true, as NVE persistently investigates procedures and business processes used by DSO (Denoted by arrow between Power and Regulatory domains on Picture 8). However direct communication might not be the most efficient, as DSOs are faced with the fact: the more information they disclose, the more regulations in return they get. One of the possible solutions would be for DSOs to have a field expert, e.g. SGSC, whom they can communicate their assumptions and considerations and only after evaluation that information can be transfered to Regulatory authorities.[18]

In other words, SGSC can be designed as a meeting place, where Power/grid companies meet Regulative authorities.

On the other hand, Commercial structure have a natural desire to know the needs of DSOs and to be able to offer their services. As DSOs are dealing with important infrastructure, they strive to be careful in choice of suppliers. Possibility to have access to the pool of competent and reliable suppliers can be implemented thorough making SGCT a market place. Performing a market place function will reflect inability of SGSC to perform consultancy as a main business activity, while ensure that service provided by contractors is at proper level of quality.

4 Conclusion

Current work was done in order to help define the position of Smart Grid Security Center (SGSC) - independent research organization- among the Smart Grid actors. Work presented detailed analysis of actors and group of actors. Analysis was based on literature review, Internet research and personal interviews. As a result we get a graph of interconnections between actors and SGCT. Edges of the graph represent relations, e.g. functional communications.

The key finding from this graph is understanding of functions of SGSC in form of meeting point between Regulative actors and DSOs, responsible for implementation. On the other hand SGSC is also a market place, where DSOs can meet reliable suppliers to hire them to solve their challenges.

Having a strong research possibility and uniting actors of Smart Grid domain, SGSC can become a scientific "umbrella" for all research and industrial activities carried out in the field.

Bibliography

[1] Whitmore, A., Agarwal, A., & Da Xu, L. 2015. The internet of things—a survey of topics and trends.

[2] Farhangi, H. 2010. The path of the smart grid.

[3] Garitano, I., Fayyad, S., & Noll, J. 2015. Multi-metrics approach for security, privacy and dependability in embedded systems.

[4] Toivanen, T., Mazhelis, O., & Luoma, E. 2015. Network analysis of platform ecosystems: The case of internet of things ecosystem.

[5] Agrell, P. J. & Bogetoft, P. 2010. Harmonizing the nordic regulation of electricity distribution.

[6] Nett, F. E. About norgesnett as. https://norgesnett.no/om-oss/#/om-norgesnett-as/. (Date last accessed Sept-2017).

[7] Skjølsvold, T. M. & Ryghaug, M. 2015. Embedding smart energy technology in built environments: A comparative study of four smart grid demonstration projects.

[8] Kristoffersen, V. Opportunities for security consultancy for fen. personal communication.

[9] KraftCERT. Services that we offer. https://www.kraftcert.no/tjenester.html. (Date last accessed Sept-2017).

[10] Kálmán, G. Mnemonic: Current goal related to security of dsos. personal communication.

[11] Oksdoel, K. Greenbird: advantages of metercloud for dsos. personal communication.

[12] Bjørk, M. Epos consulting and their services for smart grid market. personal communication.

[13] NVE. Regulations on ams and control systems. https://www.nve.no/Media/.../veiledertil-sikkerhet-i-ams.pdf. (Date last accessed Sept-2017).

[14] NVE. Regulations on ict- security. publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf. (Date last accessed Sept-2017).

[15] Myrstad, F. Forbrukerrådet taking care of consumers with installed ams. personal communication.

[16] Union, E. 2009. Directive 2009/28/ec of the european parliament and of the council of 23 april 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing directives 2001/77/ec and 2003/30/ec.

[17] Fosso, O. B., Molinas, M., Sand, K., & Coldevin, G. H. 2014. Moving towards the smart grid: The norwegian case.

[18] Duus, H. Sgsc- meeting place for smart grids actors. personal communication.