Kjell Sand, Poul Heegaard

Next Generation Control Centres – State of art and future scenarios- version 2.0

Trondheim, 2015-10-31
Next Generation Control Centres – State of art and future scenarios

ABSTRACT

The report gives an overview over control centre state of the art and possible impact of smart grid technology development for next generation control centres. Both traditional power engineering aspects are dealt with as well as the new challenges emerging when drastically increasing ICT support and automation in power system operations. Use cases as a tool for breaking down the smart grid domain in more manageable parts is addressed as well as architectural issues. A set of smart grid scenario elements is given in the report with their possible impact on next generation control centres. The scenarios are partly driven by new monitoring and control options, but also by regulatory requirements such as network codes. The scenarios are expected to give ideas on aspects to consider and thus contribute to strategy development. The report discusses Business Process Re-engineering (BPR) as a good framework for developing strategies for next generation control centres including a BPR checklist to support the strategy process.

KEYWORDS

Power System Control Centre, Smart grid, Scenarios, Business Process Re-engineering
# Table of contents

1. **INTRODUCTION** ........................................................................................................... 7
2. **ACRONYMS AND ABBREVIATIONS** ............................................................................... 9
3. **CONTROL CENTRES – STATE OF ART** .................................................................... 10
   3.1 **T&D OVERVIEW** ........................................................................................................ 10
   3.2 **CONTROL CENTRE TASKS** ..................................................................................... 11
   3.3 **EVENT DRIVEN VERSUS CONTINUOUS TASKS** .................................................... 13
   3.4 **SECURITY** ............................................................................................................... 15
   3.5 **RESILIENCE** ............................................................................................................. 16
4. **REFERENCE ARCHITECTURE AND USE CASES – SUPPORT FOR DEVELOPING NEXT GENERATION CONTROL CENTRES** ........................................................................ 18
   4.1 **SMART GRID REFERENCE ARCHITECTURE** ............................................................. 18
   4.2 **THE USE CASE APPROACH** .................................................................................... 20
5. **THE LANDSCAPE OF NEXT GENERATION CONTROL CENTRES – ARCHITECTURAL VIEW** ......................................................................................................................... 25
6. **SCENARIOS FOR NEXT GENERATION CONTROL CENTRES FOR SMART GRIDS** ................................................................................................................................. 29
7. **NEXT GENERATION CONTROL CENTRES IN THE CONTROL ROOM** ......................... 35
8. **BUSINESS PROCESS RE-ENGINEERING – A TOOL FOR RE-ENGINEERING CONTROL CENTRES** .................................................................................................................. 38
   8.1 **INTRODUCTION** .......................................................................................................... 38
   8.2 **BPR – GENERAL PRINCIPLES** .................................................................................... 38
   8.3 **STRATEGY PROCESS NEXT GENERATION CONTROL CENTRES** ................................ 39
   8.4 **BPR KEY QUESTIONS RELEVANT FOR NEXT GENERATION CONTROL CENTRES** .............................................................. 41
9. **SUMMARY/CONCLUSIONS** ............................................................................................ 44
10. **REFERENCES** .................................................................................................................. 45
1 Introduction

The NTNU project “Next generation control centres for Smart Grids” (project period 2011-2015) is targeted towards power system control centres. The planned roll out of Smart Meters, associated communication infrastructure together with more advanced sensors and controls is expected to drastically increase the amount of data and information that needs to be managed and which can be used in power system operation. The project’s main goal is to see how the increasing amount of real time and static data can be utilized more efficiently in order to operate the power system in a safer, more reliable and cost effective way.

The project targets two main areas:

- Utilization of the increasing amount of available data in order to detect, avoid and manage failures as well as to study the reliability impact of closer operational integration of electrical infrastructures and ICT infrastructures
- Management Structure for operation and maintenance in smart power grids, including proposed structure of centralized operational support and distributed automatic intelligence in order to monitor and operate smart power grids in a more reliable and cost efficient way.

Project results (reports, papers etc.) can be downloaded from the project website: http://www.ntnu.no/telematikk/projects/smartgrid/futurecontrolcenter/start

The main project financing is provided by NTNU by offering PhD and post.doc positions. In addition a number of industry partners have contributed to the project:

- Eidsiva
- Skagerak Energi
- Powel
- Smart Grid Norway
- Siemens
- ABB
- Agder Energi Nett
- Hafslund
- NTE
- EB
- Statnett
- Trønderenergi

This report is an update of a project report from 2012: Next Generation Control Centres – State of art and future scenarios NTNU IME Faculty Technical Report no. 1/2012, 2012-11-06.

The main changes from the previous version of the report are the following:

- Norwegian Smartgrid Centre projects and demonstrations descriptions have been removed as updated information is found on the centre website: www.smartgrids.no
A new chapter discussing smart grids next generation control centres from an architectural perspective is added

A new chapter describing possible new high levels tasks in next generation control centre is added

Some material have been revised based on newer versions of referenced the European Network Codes\(^1\)

Information security management is included as a new topic for next generation control centres

Some material on resilience engineering is also added together with discussing risk contribution when drastically increasing ICT support and automation in power system operations.

---

\(^1\) Network codes are a set of rules drafted by ENTSO-E, with guidance from the Agency for the Cooperation of Energy Regulators (ACER)\(^1\), to facilitate the harmonisation, integration and efficiency of the European electricity market
### 2 Acronyms and abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition – general term for industrial control centres</td>
</tr>
<tr>
<td>DMS</td>
<td>Distribution Management System</td>
</tr>
<tr>
<td>TSO</td>
<td>Transmission System Operator</td>
</tr>
<tr>
<td>DSO</td>
<td>Distribution System Operator</td>
</tr>
<tr>
<td>AMI</td>
<td>Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>AMS</td>
<td>Advanced Measurement and Control Systems – Norwegian term for Smart metering or AMI – Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>NIS</td>
<td>Network information system i.e. IT system used by mainly DSOs for network documentation including maps and diagrams, power system simulation tools, maintenance management tools etc.</td>
</tr>
<tr>
<td>DG</td>
<td>Distributed generation i.e. generation connected to the distribution system</td>
</tr>
<tr>
<td>DER</td>
<td>Distributed energy resources i.e. distributed generation and energy storage</td>
</tr>
<tr>
<td>MDMS</td>
<td>Meter Data Management System. System for validating, storing, processing and analysing large quantities of meter data.</td>
</tr>
<tr>
<td>CIS</td>
<td>Customer Information System</td>
</tr>
<tr>
<td>HES</td>
<td>Head End System. Central Data System collecting data via the AMI of various meters in its service area.</td>
</tr>
<tr>
<td>EV</td>
<td>Electrical Vehicle</td>
</tr>
<tr>
<td>PV</td>
<td>Photo Voltaic Power Generation</td>
</tr>
<tr>
<td>LV</td>
<td>Low voltage – systems or installations with nominal voltage $U_n &lt; 1kV$</td>
</tr>
<tr>
<td>MV</td>
<td>Medium voltage - systems or installations with nominal voltage $1kV &lt; U_n &lt; 36 kV$</td>
</tr>
<tr>
<td>IEC</td>
<td>The International Electrotechnical Commission. The world’s leading standardisation body within electricity and electronics.</td>
</tr>
</tbody>
</table>
3 Control Centres – state of art

3.1 T&D Overview

To establish a state of art description of the utility control centres today, visits and interviews have been made with project partners. Figure 1 gives a principle stylized presentation of the Norwegian transmission and distribution grid. Typical voltage levels are given in the figure. Connected generation and loads are not shown, but they exist on all voltage levels. At higher voltages, they are connected via a step-down transformer to adapt to the adequate voltage levels.

Secondary transformer stations e.g. typically 132/22kV or 66/11kV are well equipped with measurements and remote controlled switches and circuit breakers, while the MV distribution system feeders and distribution substations are far less equipped with only a few remotely controlled breakers. The use of fault indicators in the MV system is also limited and the LV system is mainly monitored by the customers: The utilities are made aware of LV faults by telephone calls from customers.
3.2 Control Centre Tasks

The control centres at utilities today mainly perform the following tasks:

- Grid monitoring
- Fault management
- Revision planning
- Optimising grid topology i.e. optimal configuration
- Management of customer requests and providing customer information
- Generation management to some extent
- Management of switching operations
- Operation statistics including fault and interruption statistics (FASIT)
- Change power system variables and set points (e.g. set points of regulators, voltage control, etc.)

Management of customer requests and providing customer information is typically shared with the customer call centre. The customer call centre receives all kinds of customers' requests (new connection, invoice requests etc.). Information received by the call centre that could have information value for the control centre (interruption information, outage observations, etc.) is routed to the control centre. Customer requests received outside call centre working hours are normally handled by control centre personnel. Answering machines may inform callers about known outages and expected interruption times in their area. SMS messages, internet and apps are also used to provide interruption information as shown in the examples below:

![Figure 2: Customer interruption information examples.](image-url)
The workload of the control centre varies. During normal operation the work load is not so intense. The main focus is on managing planned outages, "normal" outages, planning and documentation. But during large outages with widespread interruptions, the situation is quite stressed driven by reconnecting customers as fast as possible and in a safe way. Under such stressed situations, it is usual to call upon extra personnel to help. As personnel safety is the primary objective, work processes and responsibilities are designed for fulfilling safety requirements stated in national codes and regulations.

The most essential Norwegian regulation relating to operation of power systems is "Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg" which is largely based on the European Standard EN 50110-1:2004 Operation of electrical installations. A Norwegian version of EN 50110-1 2005 is available: "NEK EN 50110 - Sikkerhet ved arbeid og drift".

In EN 50110 operation is defined as:

\[
\textit{all activities including work activities necessary to permit the electrical installation to function. These activities include such matters as switching, controlling, monitoring and maintenance as well as both electrical and non-electrical work}
\]

The control centre is a key element in coordinating operation (monitoring, controlling, switching). Two main roles in terms of responsibilities should be mentioned:

- \textit{nominated person in control of a work activity} (Leder for sikkerhet -høyspenning/ansvarlig for arbeidet - lavspenning) defined in EN 50110 as \textit{"the nominated person with ultimate responsibility for the work activity. Some of these duties can be delegated to others as required"}

- \textit{nominated person in control of switching operations , voltages > 1kV} (Leder for kobling i høyspenningsanlegg) which has the responsibility to ensure safe switching operations.

Nominated person in control of switching operations is normally a person at the control centre, while nominated person in control of a work activity is a person at the work site. Nominated person in control of switching may sometimes be located at his office or at home.

During outages especially when many network customers are affected, the most important decision making process at the control centre is to prioritise reconnection of customers. For reconnection of customers two methods are available:

1. \textit{Rerouting} – to find alternative paths from the energy source to the customer
2. \textit{Repair} – replacement and/ or restoration of the faulty component(s)

To support prioritisation, the customers (or feeders) will be ranked according to SHE importance (Safety, Health and Environment – e.g. giving priority to hospitals etc.) or the CENS importance (Cost of energy not supplied).

One of the major changes in moving the power system in a Smart Grid direction, is the large influx of distributed generation (DG) connected to the MV or LV grid with a rating typically less than 10 MW. DG is today normally \textbf{not} monitored from the distribution system control centre. This means that information concerning the status of a DG power plant is not available in the SCADA systems. Thus, the control centre operator has not real time information concerning if the plant is running or
not, and it's actual active and reactive power input etc. Information is obtained through other channels like telephone calls. The monitoring of the LV distribution system is mainly carried out by exchanging messages (telephone calls, emails, radio, internet pages for information input from customers etc.) and not by online measurements. As stated by one project partner in a workshop:

"We are blind and happy – until the customer calls"

Monitoring of the MV distribution system is limited to the feeder bays in a secondary substations i.e. the part of a substation within which the circuit breakers and associated relay protection and monitoring equipment is contained and a few circuit breakers and short circuit indicators located at MV feeders. Some utilities have protection relays which may estimate distances to faults (short circuits) which makes it easier to locate faults.

The manpower at the DSO (Distribution System Operator) control centre is typically one or two persons outside regular working hours, but larger DSOs have backup workforce that are called upon during larger outages. It should here be mentioned that the size of the Norwegian DSOs range from less than 1000 network customers to more than 500,000 network customers. Thus, the situations may be very different from the smallest to the largest. The description given in this chapter is more adapted to larger DSOs.

### 3.3 Event driven versus continuous tasks

To analyse and map control centre tasks and activities, it is useful to have some structure according to the characteristic of the task. Some high level characteristics are suggested in the following:

The task or work processes involved in operation can be split in two:
- Continuous i.e. 24/7 tasks (e.g. monitoring..)
- Event driven or scheduled tasks (fault management, planned work…)

The control centre manages both types of work processes and a key feature separating it from most other utility work processes is the continuous 24/7 work.

From an operational or control centre point of view the work and decisions process can be structured in different ways and level of details. A suitable high-level structure is proposed below:
- Monitoring
- Planning
- Response
- Documentation

The four elements are briefly defined in the following:

**Monitoring** Situational awareness i.e. being aware of what is happening in the power system and understanding what the information means now and in the future. In practice, monitoring is done by observing power system status (measurements, alarms..) on SCADA or DMS monitors or getting information from various sources via email, telephone etc. (weather data, lightning data…).
**Planning**
Control room actions or changes in power system status will in many cases involve some planning efforts. E.g. when reconfiguring the power system topology or when isolating components for maintenance, some simulations may be necessary to ensure that power system limits (capacities, voltage limits etc.) are not violated with the new configuration.

**Response**
Actions to alarms or requests. Mostly this involves switching operations (connection/disconnection of components or loads) or change of power system variables and set points. From a control room perspective this is primarily performed by remote control or instructions to field personnel.

**Documentation**
Documentation of operation involves generation of required event logs, reports and statistics required by internal and external stakeholders (e.g. the regulator e.g. NVE, the TSO- Transmission System Operator e.g. Statnett). Fault and interruption statistics is one example (FASIT documentation).

Based on these characteristics, control centre tasks classified and analysed using the structure given in Table 1:

**Table 1 Control centre tasks - state of the art.**

<table>
<thead>
<tr>
<th>Level/phase</th>
<th>Control centre job/role</th>
<th>Cont.</th>
<th>Event driven</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Grid monitoring</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Planning</td>
<td>Revision planning</td>
<td>X</td>
<td>(X)</td>
</tr>
<tr>
<td></td>
<td>Optimising grid topology i.e. optimal configuration</td>
<td>(X)</td>
<td>X</td>
</tr>
<tr>
<td>Response</td>
<td>Remote switching operations</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Control room fault response switching operations</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manual switching operations</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fault location</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fault repair</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management of customer requests and providing customer info</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Voltage – reactive power management</td>
<td>(X)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Generation management</td>
<td>(X)</td>
<td>X</td>
</tr>
<tr>
<td>Documentation</td>
<td>FASIT</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

The (information security) incident management process, as defined by ISO/IEC 27065 [10], is comprised by five phases that is well aligned with the tasks defined for the control center. The five phases, and it’s mapping to the control center tasks are illustrated in Figure 3, and described as follows:

- **Plan and prepare** includes activities such as establishing a dedicated response team, defining roles and responsibilities, documenting procedures, as well as training of personnel and awareness raising activities regarding incident management throughout the organization.
- **Detection and reporting** is the first operational phase of incident management and involves detection of what might be an incident and reporting into an incident tracking system.
Assessment and decision phase decides what kind of response is needed to cope with the registered event.

Responses phase describes the actions taken to cope with the incident and prevent further consequences, restore systems, collect electronic evidence, and possibly escalate to crisis handling.

Lessons learned phase, the team analyzes whether the incident management scheme worked satisfactorily and considers whether any improvements are needed on any level: the scheme, policies, procedures, security mechanisms, or similar. [An important comment at this point is to also think about what we can learn from near incidents/accidents events, or events that were avoided].

Figure 3: The information security incident management process [10] combined with identified control center tasks

With the increasing imbedding of ICT in the future Smart Grids, procedures for and handling of information security incidents are required, and should be imbedded in the operations. A well-aligned procedure for incident management with the tasks and procedures in the existing call centres is therefore crucial.

The consequences will be the same: no power supplied to the consumers.

3.4 Security

According to Norwegian regulations (Emergency Preparedness Regulation – Beredskapsforskriften) [5], power system assets (including control centres) are classified with respect to their importance according the following grading:

Class 1: Assets of minor importance
Class 2: Assets of importance for the security of supply on county or sub-transmission level
Class 3: Assets of importance for the security of supply on regional, national, transmission level or for the supply of large populations, important infrastructure or other plants of special importance.
The regulations have the following special impact on control centres:

- Staffing requirements e.g. class 3 control centres should be manned 24/7 with at least two persons
- Redundancy to remotely controlled objects, e.g. class 2 control centres should have redundancy to class 2 and class 3 plants
- Admission control of personnel
- Fire security e.g. automatic fire alarms requirements
- EMP/EMI security (Electro Magnetic Pulse/ Electric Magnetic Interference.) are required for class 2 and class 3 control centres.

The security requirements and their development in view of Smart grids/Smart metering are expected to have a large impact on the degrees of freedom for provision of functions and integrations in next generation control centres. Potential socio economic benefits may not be achievable due to security constraints.

3.5 Resilience

Resiliency in (Smart) Power Grid can be defined as the ability to resist failure and rapidly recover from breakdown. A more resilient grid implies a more reliable grid.

More general, it is said that a system is resilient if it can adjust its functioning prior to, during, or following events (changes, disturbances, and opportunities), and thereby sustain required operations under both expected and unexpected conditions [12].

Resilience engineering looks at how the organization functions as a whole. Resilience engineering is a fairly recent development within industrial safety and concerns an organization’s ability to succeed under varying conditions. Hollager [12] defines four abilities of a system (technical and organizational) to described a resilient system (illustrated in Figure 4):

- **Responding (Actual)**: The ability to address the actual is knowing what to do, being able to respond to changes and disturbances in an effective and flexible matter.
- **Learning (Factual)**: The ability to address the factual is knowing what has happened, being able to learn from past events and understand correctly what happened and why.
- **Monitoring (Critical)**: The ability to address the critical is knowing what to look for, being able to monitor what can be a threat or cause disturbances in the near future.
- **Anticipating (Potential)**: The ability to address the potential is knowing what to expect, being able to anticipate developments, threats or opportunities into the future and imagine how they can affect the organization through changes or disruptions.

The basic abilities of resilience relates to the information security incident management process, and hence the tasks of the control center. Knowing what to expect (anticipation: the potential) is a result of the plan and prepare phase, where the situation awareness is developed through preparedness exercises, documentation, and monitoring. In the detection and reporting phase it is important to know what to look for (monitoring: critical), as an input to the responding phase (which defines what to do, which responses to take), combined with the results of the learning phase (where coordination is essential, Section 2.3).

The level of resilience of an organization is determined by how well these four abilities are met. A resilient organization is prepared for dealing with the unexpected and able to adapt to the occurring situations. Resilience must be developed over time. Preparedness exercises are essential in the
learning process, with cross-functional (power grid and ICT) teams and with different roles (operations, planning, business management) in the organization [13],[14].

Figure 4: The four basic abilities of resilience [12]
4 Reference architecture and use cases – support for developing next generation control centres

4.1 Smart Grid Reference Architecture

One observation after deregulation of the electricity sector in Norway in 1991 was that different work and decision making processes needed to be addressed in a more holistic way to contribute to the overall objective of the Energy law of a socio economic rational energy sector. This development was promoted by the regulator (NVE) by introducing income cap regulation and benchmarking and the CENS arrangement (CENS – Cost of Energy Not Supplied). Communication and coordination between utility departments such as the planning department, the maintenance department and the operation department came closer due to these regulatory developments. The development of smart grids, smart metering, smart houses calls for communication and coordination on a much broader and complex scale. To give an overview of the new interplay with the new assets and actors from a holistic perspective a structured framework is needed to support concept and strategy development.

The international work on smart grids has brought forward the need for so-called reference smart grid architectures. In the CEN/CENELEC/ETSI JWG report on standards for smart grids [1] the need is stated as follows:

*In essence, the purpose of a Reference Architecture is to allow for a separation of a complex system (which a smart grid definitely is) into entities that can be isolated from each other according to some principles, thus making possible the description of the whole system in terms of the separate entities and their relationships.*

An example of a high level architecture or concept is given in Figure 5: The European Smart Grid Concept developed under standardisation mandate 490

![Figure 5: The European Smart Grid Concept developed under standardisation mandate 490](image)
As indicated in the figure, the control centres as a part of operations, have an important coordination and communication function. A more detailed architecture is shown in Figure 6.

Figure 6: Smart Grid Architecture Model (SGAM) from [8].

The model consists of five layers and each layer has two dimensions:

**Domains**
Elements in the electrical energy conversion chain from large scale generation down to final user appliances

**Zones**
Hierarchical levels of power system management which considers the concept of aggregation and functional separation in power system management.

The five layers are defined as follows in [8]:

**Component Layer**
The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system actors, applications, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers.
Communication Layer
The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.

Information Layer
The information layer describes the information that is being used and exchanged between functions, services and components. It contains information objects and the underlying data models. These information objects and data models represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means.

Function Layer
The function layer describes functions and services including their relationships from an architectural viewpoint. The functions are represented independent from actors and physical implementations in applications, systems and components. The functions are derived by extracting the use case functionality, which is independent from actors. The function layer can be regarded as the use case layer (see next chapter).

Business Layer
The business layer represents the business view on the information exchange related to smart grids. SGAM can be used to map regulatory and economic (market) structures and policies, business models, business portfolios (products & services) of market parties involved. Also business capabilities and business processes can be represented in this layer. In this way it supports business executives in decision making related to (new) business models and specific business projects (business case) as well as regulators in defining new market models. The

4.2 The use case approach
On a more detailed strategy level, the use case methodology is regarded as a good approach when decomposing a system of systems which the Smart Grid definitely is. The use case methodology came from software development and is in that domain largely used to describe IT systems or programs from the customers/users perspective. The main effort was to describe functions, requirements and involved actors to ensure that the software developers (often with limited customer domain knowledge) understood well user requirements. A use case description is also used to design test requirements.

As an ICT system in general is an implementation of a set of functions, the main idea is that Smart grid also is a realization of a set of functions and thus the methodology should be applicable.

Within the area of Smart Grids, the concept of use cases and their description was adopted by Electric Power Research Institute (EPRI) and published as IEC PAS 62559 Intelligrid Methodology for developing Requirements for Energy Systems [6].

Figure 7 shows the use case approach:
The process starts with business cases expressing business needs, which motivates the needs for new smart grid functionalities and ends up with detailed technical descriptions of, use cases capturing user requirements and functionalities. Use cases play an essential role in the methodology and a use case is defined as [7]:

*Use Case: Description of the interaction between one or more actors, represented as a sequence of simple steps.*

**NOTE 1:** Actors are entities that exist outside the system ('black box') under study, and which take part in a sequence of activities in a dialogue with the system to achieve a specific goal. Actors may be end users, other systems, or hardware devices.

**NOTE 2:** Each Use Case is a complete series of events, described from the point of view of the actor.

In a Use case description the focus is on what the use case do and how involved actors affect the functionalities. How the use case is technically implemented is outside the scope. The major part of a use case description is text supported by different UML diagrams (UML-Unified Modeling Language).
The most important UML diagram is a so-called use case diagram, which gives an overview over the functionalities of the use case and the involved external actors. The figure below shows an example of such a diagram from [7]:

![Use case diagram example - Fault localization, isolation and system restoration.](image)

**Figure 8**: Use case diagram example - Fault localization, isolation and system restoration.

As developing smart grid functionalities involves many disciplines and systems, an advantage of using the use case approach is that it gives the needed overview to evaluate if all necessary building blocks and actors have been considered. An actor is defined in the use case approach as entity that communicates and interacts in a use case and is illustrated with the symbol: 

Note 1 that actors can include people, software applications, systems, databases, and even the power system itself. Many use cases have been developed the last years in various Smart grid projects and some are available in Smart grid databases e.g. EPRI's use case repository (http://smartgrid.epri.com/Repository/Repository.aspx). Such sources could provide valuable input and ideas to the development of smart grid strategies.

Another important advantage with the use case approach is that it also supports the challenge of securing interoperability in the Smart Grid, see next chapter,
IEC is now (2015) transforming the IEC PAS 62559 to an IEC 62559 Use Case Methodology series of standards with the following parts:

- **Part 1 - Concept and processes in standardization**
  This part (described in this document) of the IEC 62559 “Use case approach” provides the basis for a common use case management repository in order to gather use cases within IEC on a common collaborative platform and to organize a harmonization of use cases in order to provide broadly accepted generic use cases as basis for the further standardization work. It describes processes and provides basics for the use case approach like terms or use case types.

- **Part 2 - Definition of the templates for use cases, actor list and requirements list**
  The second part of IEC 62559 “Use case methodology” defines the structure of a use case template, an actor list and a list for requirements. The document is mainly based on the previous IEC/PAS 62559 specification and shall be read together with part 1 of this standard.

- **Part 3 - Definition of Use Case template artefacts into an XML serialized format**
  Based on IEC/PAS 62559 - part 2 this document defines the required core concepts and their serialization into XML syntactic format of a use case template, an actor list and list for detailed requirements. The XML format is used to transfer the content of the template to other engineering systems (e.g. based on UML). It is intended to develop a UML profile definition based on this part in future.

The standards will among others be used to create an IEC Smart Grid Use Case Repository that can be a useful starting point for stakeholders or projects when developing smart grid functionalities. The repository will be integrated with IECs Smart Grid Standards Map which defines relationships between components and standards of the Smart Grid. The tool is available at: [http://smartgridstandardsmap.com/](http://smartgridstandardsmap.com/). Figure 9 shows the Architecture View of the tool, while Figure 10 highlights the control centre part.
As the figures show, the model is a two dimensional version of the Smart Grid Architecture Model given in Figure 6.
5 The landscape of next generation control centres – architectural view

Based on the concepts given Figure 5 and Figure 6, Figure 11 illustrates the interaction landscape of the TSO – DSO controls centres.

Figure 11: Smart Grid Control Centre Interaction Landscape

The part of the figure highlighted with the red ellipse, marks the core control centre elements of the figure. However, as illustrated, a number of integrations and interactions with control centres are relevant.

The main terms used in the figure are explained as follows:

- **Stakeholder** - Party responsible for one or several smart grid domains
- **Smart grid domain** - Elements in the electrical energy conversion chain from large scale generation down to final user appliances
- **Smart grid zones** - Hierarchical levels of power system management which considers the concept of aggregation and functional separation in power system management.
- **Main IT systems DSO** - Main IT system categories used by the DSOs today
- **Data hub TSO** - National data hub for measurement values and market processes; such as switching of supplier, migration and reporting
The figure shows a vast number the interaction options, which adds complexity when developing next generation operation support for the smart grid. To design the overall control concept thus needs to carefully take into account the involved subsystems and their integration to facilitate the wanted smart grid functionality. Interoperability is a key success element, especially since not only in-house company systems are involved, but also a number of data exchanges take place with external IT-systems. Interoperability is defined as follows in the IEC 61850-series of standards:

**Interoperability**

*Interoperability refers to the ability of two or more devices from the same vendor, or different vendors, to exchange information and use that information for correct co-operation*

The concept is illustrated in Figure 12 from [8]:

**Figure 12 : Definition of interoperability – interoperable systems performing a function**

In other words, two or more systems (devices or components) are interoperable, if the two or more systems are able to perform cooperatively a specific function by using information, which is exchanged. The Smart Grid will thus be a system of interoperable systems; that is, different systems will be able to exchange meaningful, actionable information in support of the safe, secure, efficient, and reliable operations of electric systems. The systems will share a common meaning of the exchanged information, and this information will elicit agreed-upon types of response [9].

Interoperability is regarded as one of the most challenging issues in developing a smarter grid, as many vendors mainly support their own legacy solutions e.g. data models, data formats etc. Standardisation is the main tool to facilitate interoperability. IEC is very active within smart grid interoperability standardisation.

The core IEC interoperability standards are:

- IEC 61970: Common Information Model (CIM) / Energy Management
- IEC 61850: Power Utility Automation
- IEC 61968: Common Information Model (CIM) / Distribution Management
The objective of these standards is of course to contribute to cost effective interoperability achievement. This requires that market push the vendors to use the standards in their solutions.

It should be noted that interoperability has several aspects in is thus grouped into several layers as illustrated in Figure 13:

![Interoperability layers](image)

**Figure 13 : Interoperability layers [8]**

The same layers are found in the Smart Grid Architecture Model (Figure 6).

An example of mapping of a use case into the smart grid landscape presented in this chapter is shown in Figure 14:

![Demand Side Response - Statnett Pilot project](image)

**Figure 14 : Demand Side Response - Statnett Pilot project**
This demand side response use case is developed by the Norwegian TSO (Statnett), in cooperation with four DSOs together with SCADA and Smart metering providers. The objective of this use case was to investigate technical performance of the chain from a demand response signal was posted from the TSO’s SCADA until the demand response was reported by the TSO SCADA. For more information – see presentation:
http://www.statnett.no/Global/Dokumenter/Miljø%20og%20samfunn/Forskning%20og%20utvikling/FoU-konferansen%202015/Presentasjoner%20FoU%20konferansen%2022.-23.%20april%202015.pdf (in Norwegian).

The use case is a good illustration of smart grid stakeholder- domains-zones-systems interaction and how interoperability is dealt with using standards. To have such a structured overview supports the development of new smart grid use cases and ensures that relevant stakeholders and systems are considered.
6 Scenarios for Next Generation Control Centres for Smart Grids

To discuss next generation control centres and their role in Smart grid utilities, the overall objectives and values of the utilities needs to be addressed to clarify the role of next generation control centres in the existing and future value chains. The Norwegian deregulated power sector is divided into two main subsectors as indicated in Figure 15:

- Market
- Monopoly

![Diagram of the Norwegian Power Sector and Actors](image)

Figure 15: The Norwegian Power Sector and Actors.

The main actors related to the power system are also presented in the figure, grouped as monopoly actors and market participants.

Today, the goal of DSO control centres is to support the monopoly tasks as specified by the regulator. These tasks are according to [2]:

Grid services that comprises one or more of the following:
- Transmission and distribution of power, including operation, maintenance and investments of grid assets
- Tariffs
- Measurement, account settlement and customer management
- Installation supervision and safety
- Operations coordination
- Mandatory emergency preparedness measures
- Mandatory energy analysis
The income cap regulation for the TSO and DSOs used in Norway is designed to promote overall socio-economic efficiency. It is expected that this principles will remain stable for the years to come implying that the role of the TSO and DSOs control centres in the future also will be to contribute to the minimization of the overall grid monopoly costs. A prerequisite to determine what is a natural monopoly is the cost structure. It is not efficient to let more companies compete on performing a service when the initial cost to establish the service is high and marginal costs for increased service capacity is low. The largest part of the T&D costs relates to grid assets investment cost (overhead lines, cables, transformers…) and their associated operation costs. This cost picture is not expected to change by introducing smart grid technologies and thus not result in principle changes in the monopoly asset base and tasks. However, there may be changes in responsibilities and tasks between grid companies as observed lately in Norway:

- Sub transmission tariffs managed by the TSO (Statnett) from 1st of January 2014
- National data hub for measurement values and market processes managed by the TSO (Elhub – Statnett)
- Common Nordic end-user market where the power supplier is the single point of customer contact.

But although the main principles and objectives may be stable, new smart grid technologies and new actors will have a large impact on TSO and DSO operations and also affect the task of next generation control centres. Some main developments and characteristics are given in Table 2

**Table 2 : Scenario elements and characteristics.**

<table>
<thead>
<tr>
<th>Scenario element</th>
<th>Characteristic</th>
<th>Control centre impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart metering (AMS) in general</td>
<td>New measurements drastically increasing LV system and customer observability - Data tsunami</td>
<td>New data will offer many new control centre options (see details below in the table). Involvement of control room personnel in data collection supervision and quality assurance</td>
</tr>
<tr>
<td>Smart metering communication infrastructure</td>
<td>Substantial leap in critical, sensitive communication assets</td>
<td>Monitoring of communication status both from a reliability and vulnerability/privacy perspective</td>
</tr>
<tr>
<td>Smart metering – Earth fault monitoring</td>
<td>Recording of earth fault, time and duration in 230V IT systems. Earth fault alarms. Earth fault alarms will create a very large number of alarms.</td>
<td>Information may be managed by control centre/DMS, but is today not time critical as earth faults shall be corrected within 4 weeks. Due to the expected large number of alarms, filtering of important alarms is an issue.</td>
</tr>
<tr>
<td>Smart metering – Interruption monitoring</td>
<td>Recording of interruption, time and duration, disconnected power. Interruption alarms</td>
<td>Faster response to interruptions. More data to manage. Improved fault and interruption statistics.</td>
</tr>
<tr>
<td>Smart metering- voltage quality monitoring</td>
<td>Recording of rms voltage, rms overvoltage, voltage dips and other voltage quality phenomena, voltage quality alarms</td>
<td>Faster response to voltage quality problems and/or distribution system irregularities. More data to manage</td>
</tr>
<tr>
<td>Scenario element</td>
<td>Characteristic</td>
<td>Control centre impact</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Smart metering- customer information</td>
<td>Providing customer with energy and price information, planned interruptions, etc.</td>
<td>Control centre managing customer notification for planned interruptions and compensation for extra-long interruptions</td>
</tr>
<tr>
<td>Smart metering- other meter alarms and events</td>
<td>Recording and alarms of meter tempering attempts</td>
<td>Information may be managed by control centre, but is not time critical (?)</td>
</tr>
<tr>
<td>Smart metering- customer remote connection/disconnection</td>
<td>Option to remotely disconnect, reduce or reconnect customer load. Security issues if Smart metering systems (AMS-systems) are integrated with the SCADA or DMS system.</td>
<td>These new option will be carried out by the control centre either as an operational request for demand side management or due to commercial aspects (customer moves...).</td>
</tr>
<tr>
<td>Smart grid ICT security</td>
<td>In general, when more devices and systems are to be connected, information security is high on the agenda. Functions that may be useful to have, may meet barriers coming from the ICT-security domain.</td>
<td>E.g. barriers concerning integration between SCADA, DMS and AMS systems as proposed in the emergency preparedness regulation (“Beredskapsforskriften”). For next generation control centres, this may have a large impact on what functions that can be carried out from the control room and the possible integration of systems.</td>
</tr>
<tr>
<td>Demand response/ demand side management – DSO perspective</td>
<td>Customer flexibility options increase and is utilized on the DSO level</td>
<td>Implement demand response or demand side management schemes (direct load controls, submission of incentives/prices signals).</td>
</tr>
<tr>
<td>Demand response/ demand side management – TSO perspective</td>
<td>Customer flexibility options increase and has aggregated use on the TSO level</td>
<td>Need for increased exchange of data between the control centres of the DSO and the TSO to monitor and mobilize flexibility for system needs.</td>
</tr>
<tr>
<td>EVs/PHEVs</td>
<td>Slow charging and fast charging stressing distribution grids and may create congestion</td>
<td>Monitor and manage charging to maintain distribution system capacity and voltage quality</td>
</tr>
<tr>
<td>Distributed generation behind the meter (&quot;Plusshus&quot;)</td>
<td>Micro generation – mostly rooftop PVs</td>
<td>Monitor distributed generation for operational reasons and for safety during grid maintenance work. DSO control centre sets control parameters for local generation.</td>
</tr>
<tr>
<td>Scenario element</td>
<td>Characteristic</td>
<td>Control centre impact</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Distributed generation connected to LV and MV</td>
<td>Small scale generation normally &lt;10MW – mostly hydropower with limited reservoirs</td>
<td>Monitor distributed generation for operational reasons and for safety during maintenance work. DSO control centre sets control parameters for local generation.</td>
</tr>
<tr>
<td>Distribution Management Systems (DMS)</td>
<td>ICT system supporting distribution system operation</td>
<td>New tool in the control centre as an information hub for &quot;all&quot; new &quot;smart grid data&quot;</td>
</tr>
<tr>
<td>Smart fleet management</td>
<td>Use of vehicle tracking systems by GPS or similar to operate field service resources (cars etc.) for fleet management functions such as fleet tracking, routing, dispatch, on-board information and security.</td>
<td>Control room personnel may rapidly dispatch resources (cars, cranes, people, tools..) to respond to outages, alarms etc. via SMS, telephones, radio, in car displays/ software..</td>
</tr>
<tr>
<td>New sensors and meters in distribution substations – breaker status information</td>
<td>Breaker status remotely available for switches/breakers in the distribution substation</td>
<td>MV and LV distribution system topology available in close to real time.</td>
</tr>
<tr>
<td>New sensors and meters in distribution substations – alarms</td>
<td>Interruption alarms, earth fault alarms, neutral protection device (&quot;disneuter&quot;) alarm, voltage quality alarm, substation condition alarms (open door, water, temperatures), short circuit indicator alarm…</td>
<td>Monitoring and management of time-critical and non-time-critical alarms</td>
</tr>
<tr>
<td>Increased use of remote imaging and sensing</td>
<td>Fixed and mobile cameras and other equipment (e.g. thermographic equipment) that provide images and videos. Drones have been more common to carry such equipment.</td>
<td>Remote presence gives better situational awareness, but more information to manage.</td>
</tr>
<tr>
<td>Distribution system self-healing systems</td>
<td>Transferring customers to an optional power source when their normal supply has been lost. Optional sources may include neighbour feeders and Distributed Generation (DG). Personnel safety is an issue as well as secure and reliable communication during outages.</td>
<td>Reduced workload during faults to coordinate manual switching to locate faults and restore supply. New systems and information to monitor. One challenge is to update control rooms personnel with the response of any automation i.e. the role of operators in semi-automated control loops.</td>
</tr>
<tr>
<td>Virtual Power Plants (VPP)</td>
<td>A VPP is an aggregation of several DGs and operated as a single power plant.</td>
<td>Manage information for aggregated DG in the control centre area.</td>
</tr>
<tr>
<td>Scenario element</td>
<td>Characteristic</td>
<td>Control centre impact</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Microgrids</td>
<td>A microgrid is connected to the MV or LV distribution system as a single &quot;load point&quot;, contains DG and loads and can be operated in islanded mode.</td>
<td>Monitor distributed generation for operational reasons and for safety during maintenance work. Implement micro grid demand response or demand side management schemes. Reduced priority during outages.</td>
</tr>
<tr>
<td>Grid connected energy storage</td>
<td>Grid connected energy storage e.g. batteries are becoming more common and might serve various purposes such as power quality conditioning, reserves during outages, etc. Batteries might be an element in a microgrid.</td>
<td>Energy storage as an active asset in the power system needs to be monitored and managed from the control centre to secure optimal utilization and safety.</td>
</tr>
<tr>
<td>Smart homes</td>
<td>Interfaces with smart homes will facilitate demand side management/demand response options, smart charging of EVs, monitoring of DG etc.</td>
<td>Control centre impacts are already covered under the more specific topics smart houses facilitate.</td>
</tr>
<tr>
<td>Regulatory development: ENTSO-E Network Code for Requirements for Grid Connection Applicable to all Generators</td>
<td>Excerpt from the code: <em>Type B requirement: Power Generating Facilities shall be capable of exchanging information between the Power Generating Facility Owner and the Relevant Network Operator and/or the Relevant TSO in real time or periodically with time stamping as defined by the Relevant Network Operator and/or the Relevant TSO. A Power Generating Module is of Type B if its Connection Point is below 110 kV and its Maximum Capacity is at or above a threshold of 1.5 MW in the Nordic Countries</em></td>
<td>Most small DG plants connected to the distribution grid will may be monitored from the SCADA and or DMS system giving better safety and operational control. More data to manage.</td>
</tr>
<tr>
<td>Scenario element</td>
<td>Characteristic</td>
<td>Control centre impact</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Regulatory development: ENTSO-E Draft Network Code for Operational Security</td>
<td>Excerpt from the draft code: Real-Time data exchange between TSOs and DSOs within the TSO’s Responsibility Area 1. Each DSO shall provide in real-time to its TSO the information related to the Observability Area referred to in Article 19(1) and Article 19(2), comprising: a) actual substation Topology; b) Active and Reactive Power in line bay; c) Active and Reactive Power in transformer bay; d) Active and Reactive Power injection in Power Generating Facility bay; e) tap positions of transformers connecting to the Transmission System; f) busbar voltages; g) Reactive Power in reactor and capacitor bay; h) best available data for aggregated generation in the DSO area; and i) best available data for aggregated consumption in the DSO area.</td>
<td>The export of data from the DSOs SCADA and DMS system is expected to drastically increase based on this requirement. Topology information export may be more complicated than the export a pure measurement data.</td>
</tr>
<tr>
<td>Increased system complexity</td>
<td>As smart grid is a system of systems with an increasing number of systems, interactions and data, system complexity will increase</td>
<td>It is a challenge for next generation control centres to design a robust control hierarchy that keeps control room personnel in the control loop with sufficient situational awareness and instruments for control actions</td>
</tr>
</tbody>
</table>
7 Next Generation Control Centres in the Control Room

The utility control centres today in Norway often have several “control centres” in the same control room. E.g. with some of the larger utilities, the control room could host:

- Control Centre for Generation
- Control Centre for HV sub transmission (in Norwegian: regionalnett)
- Control Centre for the Distribution System
- Control Centre for the District Heating System

The smart grid development in direction of a “system of systems”, conceptually it is useful to discuss a number of new control centres in the control room for various monitoring and control of even more systems or subsystem. The term *control room* is here not necessarily used to describe a physical room or place, but is a collective term for the 24/7 operations of the utility. Based on the scenarios given in chapter 6 and discussions with project partners, the following list of possible control centres for the smart grid was developed:

- Transmission System Control Centre
- Sub-Transmission System Control Centre (“Regionalnett”)
- Large Scale Generation Control Centre (typically units larger than 10 MVA)
- District Heating Control Centre
- MV Distribution System Control Centre
- LV Distribution System Control Centre
- DG Control Centre (MV, LV, prosumers)
- Demand Side Management Control Centre (HV, MV, LV)
- Microgrid Control Centre
- Energy Storage Control Centre (e.g. battery management)
- Communications System Control Centre
- Meter Data Management Control Centre (e.g. smart meter data management)
- EV Charging Control Centre
- Power Quality Control Centre
- Earth Fault Control Centre
- Maintenance Management Control Centre (e.g. monitoring condition data for preventive actions)
- Smart Distribution Substation Control Centre (MV/LV substation)
- Network Customer Control Centre (e.g. for auto registration of customers and changes in customer installations).

The elements shown in bold are largely new elements resulting from the possible smart grid development scenarios described in chapter 6. The elements existing today (not in bold) should to some extent be reengineered adapted to the smart grid environment – e.g. to manage new tasks and new data. The demand side response use case described in Figure 14 is an example of new functionalities to implement in the Transmission System Control Centre.

The future Smart Grid will involve both old and new stakeholders, and their roles for the traditional companies (e.g. DSO, TSO) might be changing. So, it is not straightforward to identify which “control centres” the different parties will need in the future for their daily operations. Some of the
elements listed above, might be needed by several parties. E.g. the “Demand Side Management Control Centre (HV, MV, LV)” might be relevant both for the TSOs, DSOs, aggregators and power suppliers so the technical functionalities might be duplicated, but for different purposes. The TSOs and DSOs might limit the use of demand response for power system emergency operations, while aggregators and power suppliers might use demand response for smart operations.

With the increased use of intermittent distributed generation, demand side flexibility, system automation as well as market influence on power system state, next generation control centres need significantly improved information, visualization and decision support to make control centre operators aware of system state and of potential threats, and informed of the suitability of potential interventions to emerging critical situations.

With more “real time processes” e.g. real time pricing and access to massive quantities of real time data, to ensure that the control room operator is provided with the optimal information of the state of the system and of the possible control actions to enable taking preventive or corrective actions, in order to maintain or return the system in safe state of operation, is a huge challenge.

To balance speed of response, degree of automation and safety is crucial as the possibilities of faster interventions from operators or more pervasive automation increases. Personnel safety is always the top priority with utility, but there is always a trade of between safety and more efficient operation. A good example of such a trade of is the so-called self-healing grid (SHG). SHG is a system comprised of sensors, automated controls, and advanced software that utilizes real-time distribution data to detect and isolate faults and to reconfigure the distribution network to minimize the customer interruption time. The use of automated operation of switches and circuit breakers to quickly isolate the faulted section of the feeder and re-establish service to as many customers as possible, will reduce the costs of interruptions both for the customers and the DSO (reduce the Cost of Energy Not Supplied – CENS Norwegian: KILE). But such automated response might increase the safety hazard for personnel if the operators don’t have a good understanding of the fault conditions.

The imbedding of power grid and ICT systems will make the operation of the network more efficient. It will enable more timely and precise knowledge and information about the grid system state, to facilitate timely (proactive) maintenance, and reduce the frequency and consequences of failures, e.g., by reduced outage time due to short detection and localization times, and that an appropriate action (response) can be taken automatically or manually and remotely executed. This implies that new (ICT) functionality is added and new technology is included in the operations, which is new to the control center operators, and might change the workflows.

Figure 16 illustrates a risk curve where the events with high ”probability” have low consequence, and the events with low ”probability” have high consequence. The introduction of ICT-based support system, to operate a critical infrastructure such as Smart Grid, is expected to reduce the consequences and probability of daily events. Less human resources are needed for the daily operations. However, due to the introduction of another ICT-based system, the complexity and interdependency in the total system will increase, with the potential consequence of increased probability of critical events with extensive, and long lasting consequences. Such events affect large parts of the system, and take long time to recover from because of lack of understanding of the complexity (“we have not seen this failure before”), or the lack of maintenance support and coordination between the different subsystems and domains in the digital ecosystem (“who should do what?”). As indicated in the figure, it is not only necessary to increase the focus and man-
power on the events with larger consequences, but also increase the competence of the operation personnel.

**Figure 16: Introducing ICT support to assist daily operations might increase the overall risk [11]**

Another consequence of the introduction of ICT system in the power grid is the increased information security vulnerability. With multiple control centers (virtual or physical) to operate different functions, it is crucial to have well-functioning cross-functional teams that are prepared for handling failures and indicants that affects several of the functions, so coordinated actions must be taken to recover. It is important to have cross-functional preparedness exercises, and carefully debrief and learn from it [13], [14]. The same have to be done after real events (such as failures or security incidents), and after “near events” and events that was prevented.
8 Business process re-engineering – a tool for re-engineering control centres

8.1 Introduction

The project is based on the general expectation that the deployment of Smart Meters and new sensors will drastically increase the data volume to be managed by Distribution and Transmission System Operators. This will in turn trigger the necessity of rethinking or reengineering many work processes within the utilities and their management and organisation. New strategies need to be developed. To support this, the scenario elements given in Table 2 form a basis for discussion and in this chapter, some high level strategic questions and possible solutions are discussed. Such a high level forward thinking activity is necessary to identify relevant problems and options in order to shape the next generation control centre. Business process re-engineering (BPR) is a good framework for the discussion of next generation control centres.

8.2 BPR – general principles

BPR began as a private sector technique to help organizations fundamentally rethink how they do their work in order to dramatically improve customer service, cut operational costs, and become world-class competitors. BPR is basically rethinking and radically redesigning an organization's existing resources and find if additional resources are beneficial. As stated above, the requirement to implement smart metering is providing new resources (and new tasks) to the utilities. Thus, the reengineering process is already under way.

Reengineering starts with a high-level assessment of the organization's mission, strategic goals, and customer needs. Basic questions are asked, such as "Does our mission need to be redefined? Are our strategic goals aligned with our mission? Who are our customers?" Only after the organisation rethinks what it should be doing, does it go on to decide how best to do it [3].

Within the framework of this basic assessment of mission and goals, re-engineering focuses on the organization's business processes—the steps and procedures that govern how resources are used to create products and services that meet the needs of particular customers or markets. Re-engineering identifies, analyses, and re-designs an organization's core business processes with the aim of achieving dramatic improvements in critical performance measures, such as cost, quality, service, and speed [3].

Re-engineering recognizes that an organization's business processes are usually fragmented into sub processes and tasks that are carried out by several specialized functional areas within the organization. Often, no one is responsible for the overall performance of the entire process. Re-engineering maintains that optimizing the performance of sub processes can result in some benefits, but cannot yield dramatic improvements if the process itself is fundamentally inefficient and outmoded. For that reason, re-engineering focuses on re-designing the process as a whole in order to achieve the greatest possible benefits to the organization and their customers. This drive for realizing dramatic improvements by fundamentally re-thinking how the organization's work should be done distinguishes re-engineering from process improvement efforts that focus on functional or incremental improvement.
As indicated in Figure 17, work processes, information needs, and technology are interdependent. When a reengineering project leads to new information requirements, it may be necessary to acquire new technology to support those requirements. It is important to bear in mind, however, that acquiring new information technology does not constitute reengineering. Technology is an enabler of process reengineering, not a substitute for it. Acquiring technology in the belief that its mere presence will somehow lead to process innovation is a root cause of bad investments in information systems.

The Clinger-Cohen Act seeks to remedy this by insisting that process redesign drive the acquisition of information technology, and not the other way around. (The Clinger–Cohen Act (CCA), formerly the Information Technology Management Reform Act of 1996 (ITMRA), is a 1996 United States federal law, designed to improve the way the federal government acquires, uses and disposes information technology – Source: Wikipedia).

8.3 Strategy process next generation control centres
To develop a good strategy for next generation control centres a clear mission statement is the starting point followed by explicit formulation of values and objectives. To decide what is a good strategy is a consequence of these statements. Often (in a creative engineering environment), too little time is spent on these issues as it is much more fun to develop ideas and concepts for solutions. But if a problem is diffusely defined, a suggested solution may not be the best solution for the real problem.

Strategy development may be considered as a problem solving process and the OFPISA-model is a good mental framework. The OFPISA model is also referred to as Creative Problem Solving
Process CPS) or Osborn-Parnes CPS process. The process is explained below and extended with two more steps (OFPIEAM).

The model includes eight steps:

- **O** - Objective
- **F** - Fact (Status)
- **P** - Problem = O-F
- **I** - Ideas, alternatives
- **S** - Solution
- **A** - Accept
- **I** - Implement
- **M** - Monitoring results – mapping against plans, taking corrective action which may imply amending objectives/strategies

The model is shortly explained in the following:

A strategic problem is often triggered internally by the fact that the existing situation should be improved, or externally by changes in the business framework (regulations, changes in customer requirements etc.). SWOT analysis (Strengths, Weaknesses/Limitations, Opportunities, and Threats) is a popular tool for identifying internal and external factors that are favourable and unfavourable to achieve overall vision and mission and as a source to set new objectives. Also developing scenarios is useful to discuss possible futures and the challenges and opportunities that may arise (as an example, see the list of scenario elements given in Table 2).

As indicated in the process description above, the Problem (strategic problem in this context) is defined as the difference between the Objective(s) and the Fact(s). If the gap is large, it is an indication that the problem is worthwhile to address. If the gap is zero, the problem is non-existent. A primitive example could be that the regulator requires an average response time to power interruptions of less than one hour. A utility analyses the fault and interruption statistics which shows that the average response time is 55 minutes. The performance (Fact) is better than the requirement (Objective) thus the utility don't have a problem with this new requirement.

If the problem exists, the next step is to develop ideas and alternatives to close the gap between Fact and Objective. Many brainstorming techniques exist to support this step.

**Solution:** In a decision making process certain decision criteria need to be formulated as a tool to choose among alternatives. An objective function is a mathematical formulation of such a criterion. One definition of the term objective function is:

A function associated with an optimization problem which determines how good a solution is.

An objective function is for instance: “Minimize socio-economic grid costs (CAPEX+OPEX)”.

The overall objective as stated in the Norwegian Energy Act is to ensure that generation, conversion, transmission, trading and distribution of energy are rationally carried out for the benefit of society, regarding both public and private interests affected. This means that decision making should have an holistic approach, implying that all costs and impacts related to the energy system for all stakeholders should be considered, not only those being part of the corporate economics.
This objective can be met by applying socio-economic planning principles and analysis when choosing among alternatives [4].

The following main criteria are important to fulfil in socio-economic analysis:

1. All relevant alternatives should be evaluated
2. All relevant impacts of the different alternatives for all stakeholders affected should be included. This means that performance indicators are needed to evaluate different impacts. (CENS – Cost of Energy Not Supplied is an example of a performance indicator.)
3. The different alternatives should be compared with the reference alternative which may be the existing system solution (including the “do nothing” solution).
4. It is recommended to seek possibilities for flexible and robust solutions with respect to the uncertainties involved and to seek optimal timing of the implementation.

When the best Solution(s) are identified, it is important to prepare for Acceptance among the stakeholders affected. Especially internally when control centre tasks are added or changed, the people at the control centre should be consulted before implementation. The best Solution is hard to implement if it is not understood and supported by the control centre personnel.

A successful Implementation of a new control centre solution requires that necessary resources (time personnel, money) and training are available. Good training is a key element to reengineering success.

In the operational phase, it is important to Monitor performance to evaluate if the reengineering was successful or if adjustments are needed. If it needs to be adjusted, it is the same as accepting that the Objective and the Fact don't match and a "new" Problem is identified. A "new" reengineering process can be started.

8.4 BPR key questions relevant for next generation control centres

As stated in 8.2 process re-engineering should lead to the possible acquisition of new resources such as ICT-tools like DMS and not the other way round. But as implementation of Smart metering (AMS) is mandatory and will be a new resource and a new challenge for the control centres, the BPR hen-and-egg principle is somewhat distorted. Though, many of the basic questions from BPR will still be very valid for developing new strategies for next generation control centres and are listed in the following (for general details, consult [3]) .

The assessment questions deal with issues and activities that reengineering practitioners have found to be critical in defining reengineering opportunities and goals, ensuring that reengineering projects are well managed, maximizing the return on resources invested in reengineering (including information systems), and managing the many changes needed to implement a redesigned work process. The list is valid as a check list. Thus all assessment issues (questions) should have a positive answer if a reengineering project is expected to be implemented successfully. (It is noteworthy that the checklist is well in line with the OFPISAIM concept.)

1. Has the TSO/DSO reassessed its mission and strategic goals?
   As smart metering and other smart grid technologies are available (and partly mandatory), there is a need and an opportunity to address mission and vision both for the grid company
2. **Has the TSO/DSO identified performance problems and set improvement goals?**
   Any business can improve and to identify where improvement may have a potential, to document and benchmark performance are useful. It is recommended in [3] to establish ambitious performance improvement goals that are mission-oriented and meaningful to customers and stakeholders and to select and prioritize processes to be improved.

3. **Should the TSO/DSO engage in reengineering?**
   There is a need to assess the DSOs/TSO's readiness to engage in a reengineering project and to integrate the reengineering project into the utilities overall strategy for improving mission performance. Develop and begin implementing a change management plan to overview what is required. As many utilities in Norway are small, it is wise to be critical to the utilities ability to acquire and implement smart grid reengineering technologies and work processes. To waist money and time on an unsuccessful reengineering project may be worse than doing nothing.

4. **Is the reengineering project appropriately managed?**
   When a reengineering project has been launched, it should be followed up on a company executive level. Key activities are:
   - Establish an executive steering committee and project sponsor to support the reengineering project.
   - Establish an owner for the process to be reengineered.
   - Form a qualified, trained, well-led team to reengineer the process and its supporting structures.
   - Establish a clear team charter that defines project goals, resources, constraints, and deliverables.

5. **Has the project team developed feasible alternatives?**
   - Create alternatives
   - Design alternatives and test their effectiveness through simulations and/or limited pilots.
   - Assess the impact of potential barriers to implementing alternatives.
   - Develop a performance-based and risk-adjusted benefit-cost analysis of each alternative (CAPEX, OPEX and other performance indicators).

6. **Has the project team completed a sound business case for implementing the new process?**
   - Select a feasible alternative with a high socio-economic return on investment.

7. **Is the TSO/DSO following a comprehensive implementation plan?**
   - Establish a transition team and develop a comprehensive plan to manage implementation.
   - Manage training and workforce redeployment issues.
   - Conduct pilot tests of the new process prior to full implementation.
8. Are TSO/DSO executives addressing change management issues?
   1. Prepare and follow a change management strategy.
   2. Encourage staff to accept new ideas and adopt the new process.
   3. Prepare staff, managers, and executives for changes in their roles and career expectations.

9. Is the new process achieving the desired results?
   This is the same as the Monitoring results in the OFPISAIM model:
   - Measure the performance of the new process.
   - Determine if the new process is achieving the desired results.
   - Use performance measurement as a feedback loop for continuously improving the new process.
9 Summary/conclusions

Smart grid technologies are expected to have a major impact on the future development of the electrical power system. All power system domains will be affected, but the largest changes may take place in power system operations and control centres which in some of the scenarios will be the main hub for:

- Monitoring
- Planning (operational)
- Response
- Documentation

of the Smart grid as the power system develops into a more online and real time system – especially at distribution levels.

To develop robust strategies to meet the possible scenario elements described in the report is not trivial and will take large efforts. As technologies, opportunities and barriers are expected to change with time, the strategy development task is demanding also from the perspective of aiming at a moving target.

But strategy development should start on many levels – also at control room level, so the investments needed today to fulfil AMS/Smart metering requirements also are future proof and will contribute to meeting more long term objectives.

The scenario elements given in the report are intended to give input to strategy discussions and development. The BPR methodology and check list are regarded as relevant tools for strategy development. It is recommended to step-wise develop sub strategies that fit into an overall master strategy. High level use cases are one option to decompose such a master plan into sub-strategies.
10 References


