General outline SmartGrid Security Centre

A premise for the transition to the SmartGrid era is the implementation of Automatic Meter Reading (AMR) at all power-consumers in the grid. In Norway this will be fully implemented by January 1st 2019, and thus connecting society's arguably most critical infrastructure to the internet. With cyber-attacks on businesses and infrastructure on the rise, a proper framework and support-structures to ensure continued system-security is needed.

One aim of the IoTSec-project is to create and run a SmartGrid Security Centre (SGSC), in order to facilitate and aid with security testing and -development for the concerned parties. It will function as a centre of expertise and consulting body for Distribution System Operators (DSO). Through this Centre the DSOs will pave the way towards a secure- and privacy-aware Smart Grid infrastructure, harvest experiences from each other, meet with IT security experts and academia and get assistance with relevant security issues.

The Security Centre aims at becoming a National Focal point for Security in Smart Grids, by creating a common platform for both the industry and academia, and involvement of relevant parties and contributors. These would typically include national, and potential foreign DSOs, telecom-companies, governing and regulatory-bodies such as NVE and Datatilsynet, universities and third-party service providers such as eSmart Systems. This is not an exhaustive list, but an indication of what partners one would expect to find cooperating in the Security Centre.

Acknowledging that IoT and Smart Grid Security are broad topics, the establishment of the centre will be two-parted. The first phase will focus on the grid as it is today, with the implementation of AMR, and what challenges and possibilities this opens for the DSOs. The second phase will include topics such as smart housing and prosumers to the SGSC. In the following, the first phase will be in focus, as it is the most pressing matter at hand.

Recent incidents in the grid indicate that security is one of the dominant issues to be addressed. In addition to being a consulting body on Smart Grid Security, the Centre can provide penetration-testing of security-systems, followed by an extensive analysis, and recommendations to possibly improve system security for the individual DSOs. For interested parties, the Centre can also provide full scale tailored system security solution, in addition to assist in smart utilization of the Big Data collected by DSOs. A long-term goal is to develop a system security certification, giving an indication that the system is at the very least according to standards and regulation set by governing bodies.

Seeing that weak links in the security-chain include the human interaction with the system, and that social engineering is becoming a real threat, the human involvement is going to be addressed. The Security Centre will provide awareness-training and courses for critical staff and partners, to minimize the risk they pose to the system, and to increase the likelihood that they will withstand possible attackers.

In the second phase, the SGSC will add competence and services on smart housing and prosumers to its portfolio. This could include aspects such as privacy-aspects of information-flows, new functionality and services within the smart home, and smart loads that responds to fluctuation in energy-prices. The security- and privacy threats the prosumer poses to the utility could also be evaluated in this phase.

To ensure a vivid and active environment, gatherings and happenings will be organised at the Security Centre, connecting the academia, industry and other parties onsite. Typical activities could be regular workshops for DSOs and academia, professional hacking events, or hosting national conferences on IoT-security and related topics.

Figure 1 indicates the typical elements of the envisaged smart grid. The figure focusses on system elements, and indicates the communication between the elements.

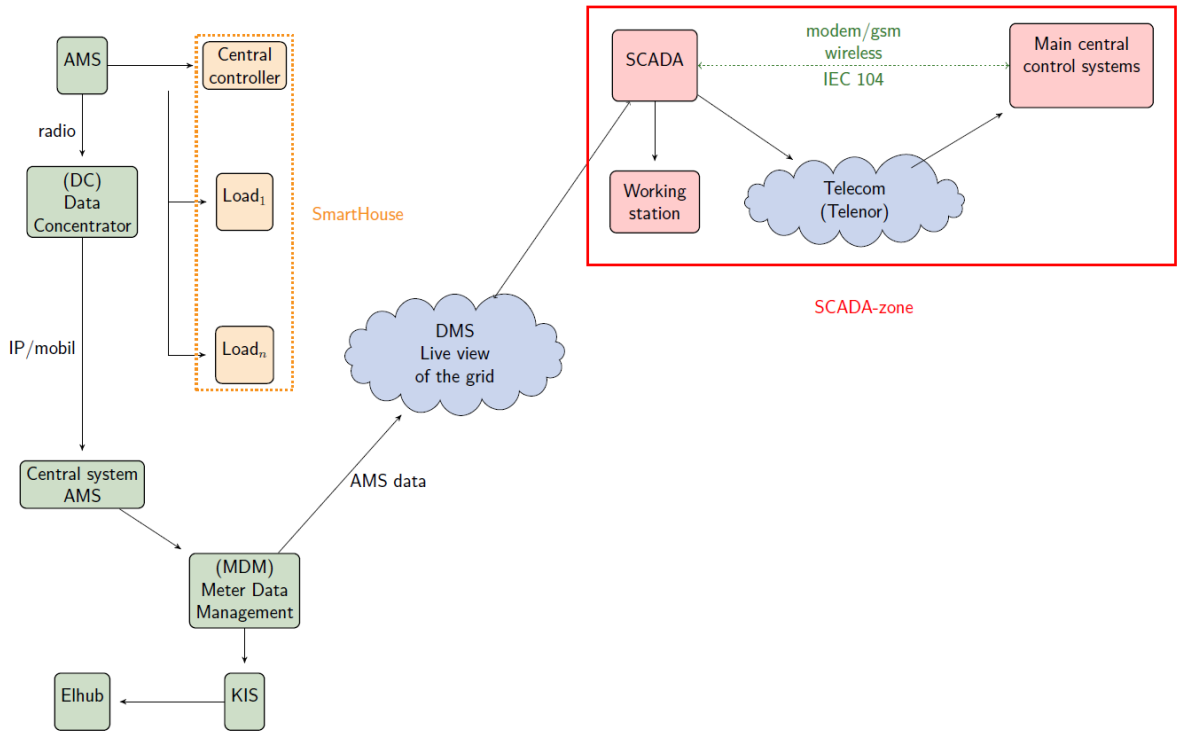

Figure 1 - Smart Grid infrastructure elements

Knowing that security issues are mainly linked to attacks on the information interfaces, an example of the service portfolio of the Security Centre is as follows:

1. Create an information flow model of the smart grid infrastructure, based on the existing functional overview.
2. Annotate the information flow model with specific information relevant for a security analysis, a.o. create the semantic system model
3. Analyse the information flow model with respect to security threats, and provide recommendations
4. Suggest state-of-the-art technologies to cope with a certain threat environment
5. Involve employees into security trainings
6. Establish real-world security measures, e.g. penetration testing
7. Provide a roadmap towards enhanced and innovative service environments

This specific example of a service provided by the Security Centre is taken from ongoing discussions with municipalities and DSOs. The Centre expects to build a more complete service portfolio within the first years.