THE ELECTRICITY SYSTEM OF THE FUTURE (SMARTGRIDS) AND SECURITY OF ELECTRICITY SUPPLY

Senior Research Scientist/Professor II Gerd H. Kjølle,
SINTEF Energy Research & Dept. of Electric Power Engineering, NTNU
Contact: gerd.kjolle@sintef.no

Smartgrids are the vision for the future electricity system. It is an electricity grid that can intelligently integrate the actions of all users connected to it – generators, consumers, and those that do both – in order to efficiently deliver a sustainable, economic and secure electricity supply. Smartgrids utilize information and communication technology (ICT) for new measurement and control, including demand side management.

Advanced measurement and control systems (AMS) and communication with all grid customers and apparatus play important parts in smartgrids. AMS means that all households get a smart meter which registers the electricity consumption on an hourly basis and automatically submits the data to the network company. In Norway, all electricity customers will have a smart meter installed by 2019.

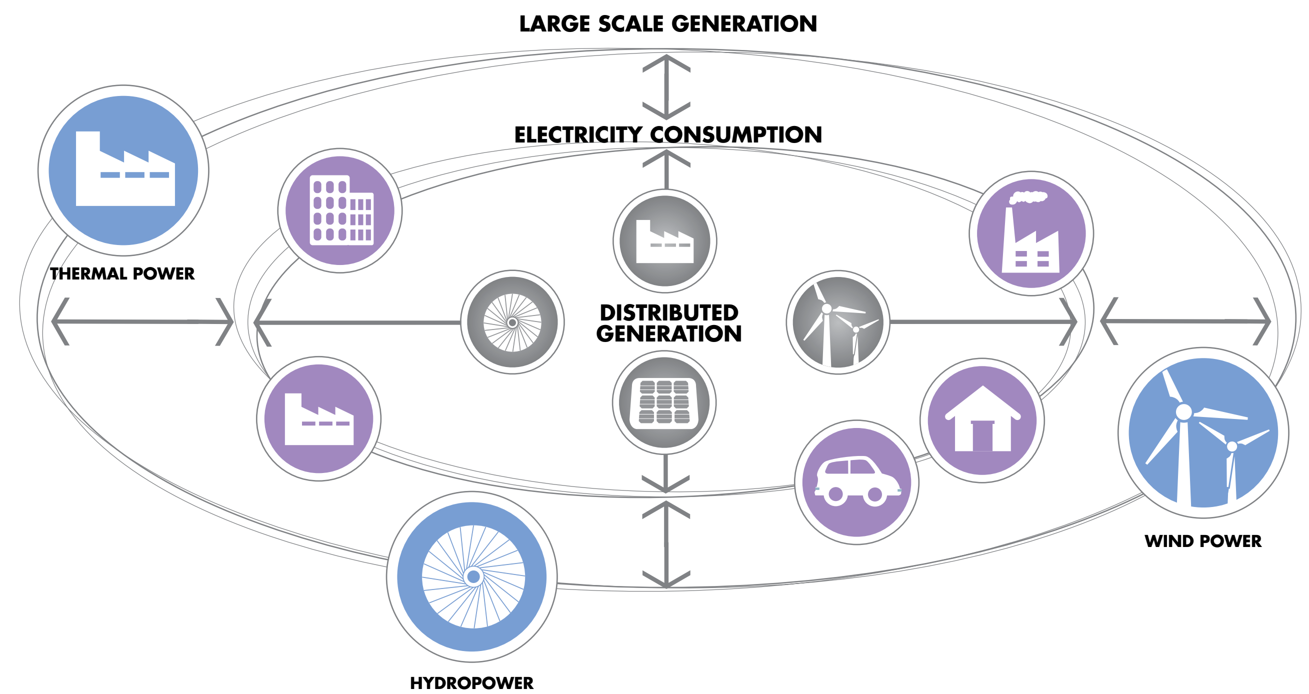
One target of the European Commission is that by 2020, 50% of the European power grids will be operated according to smart principles. Even if there are smart technologies already in place, the smartgrids will evolve gradually along with necessary development of the electricity grids. The current electricity system is an ageing infrastructure and the need for re-investment is rapidly increasing. Low levels of investment compared to the increase in electricity consumption have led to increased loading degree of components and higher utilization of the installed capacity in electricity generation and grids. At the same time climate change may impose increased weather-related stress on the grids. However, the robustness and availability of the electricity system are high in the current situation: we experience on average about two – three hours of electricity interruptions per year.

Climate change is one of the major drivers for the evolution of smartgrids. Fulfilment of strategies for massive integration of large-scale renewables and intermittent distributed generation, e.g. from wind and solar energy, as well as energy efficiency and electrification of transport, imposes new requirements on the electricity system. There is a need for changes in the development and operation of the system as the current system is built for the traditional power flow from large sources to demand. Security of electricity supply is another important driver for change. Society is critically dependent on a secure electricity supply to maintain its functionality and cover basic needs such as food and water supply, heating, safety, financial services, etc. Security of electricity supply means the ability of an electricity system to supply end customers with electricity. It is composed of a secure energy supply and sufficient power capacity, as well as reliable components and installations, to produce and transmit the electricity. Society's dependency on electricity will increase as a consequence of more use of ICT and new uses like smart meters, electrical vehicles and distributed electricity storage.

Smartgrids provide opportunities for securing the electricity supply. The availability of new and more widely distributed energy sources gives flexibility in the generation of electricity and a higher degree of energy security. Smart meters with two-way communication (AMS) may give increased consumer flexibility and possibilities for reduced peaks in electricity prices. AMS may also provide incentives for reductions in electricity consumption and possibilities for load control. Controlling individual loads and devices provides opportunities for differentiating the security of electricity supply, thereby prioritizing critical loads and functions. In periods of grid congestion, load control can relieve the congestion and the loads can be utilized as ancillary services in the regulation of the electricity system. Moreover, measurement and sensor technologies provide better possibilities for condition monitoring and improved documentation for grid operators and for maintenance and renewal of components and installations. Evolving failures may be detected and handled before they eventually lead to disturbances, and thereby reducing electricity interruptions. Alternatively, if interruptions occur the equipment may provide rapid fault detection and restoration of supply. Access to more energy sources combined with storage and load control provides better reserve possibilities in case of electricity interruptions.

Smartgrids introduce several challenges that need to be dealt with to secure the electricity supply. The current electricity grid is not built for the visions of smartgrids. The electricity system of the future should be designed in such a way that reinvestments are made smart. Better planning and new ways of operating the system are needed to ensure robust interoperability of the various parts of the system. Smartgrids involve increased complexity, more uncertainties and interdependencies on other infrastructures (ICT in particular, and transport). The dependency increases to well-functioning control and automation systems, and small disturbances may propagate to other infrastructures due to tight couplings.

The realization of smartgrid's functionality is a big leap in the integration of ICT on all levels of the electricity system, representing a fusion of the electricity grid and the Internet. New types of failure and threat are thereby introduced, such as cyber-attacks, software failures and drastically increased amounts of data in the operation of the electricity system. A data failure might, for instance, lead to a lack of overview and control of the situation. This might further lead to electricity interruptions and increased time for restoration of the electricity supply.



While the reliability and robustness of the power system in general are expected to increase with new investments and smarter grids, the risk of extraordinary events (with a low probability of occurring) might increase due to vulnerabilities caused by dependencies, increasing complexity, new components and technologies, cyber threats, new operating scenarios, etc.

Huge investments are needed for the realization of smartgrids. In Norway alone, the transmission system operator Statnett is planning for investments in the order of NOK 50 – 70 billion up to 2020. The total grid investment plans for all grid levels in Norway add up to 130 billion NOK for the coming 10-year period, including smart meters and interconnections to other countries. In addition, there are plans for new power plant investments in the order of 40 – 50 billion NOK.

Various technological, societal and economic challenges need to be overcome if the visions of smartgrids are to be realized. The social acceptance of building new infrastructure must be increased and huge efforts are needed in research and development, demonstration and innovation.

These challenges need multidisciplinary solutions. In particular, methods should be developed to analyse the impact of the challenges for the security of the electricity supply, where different elements can be dealt with in a holistic way, i.e. interaction between energy availability, capacity and failures in the electricity system. Smartgrids also increase the need for cross-sectorial risk and vulnerability analyses focusing on new types of undesired events and interdependencies.

More information about smartgrids can be found on the website of the Norwegian Smartgrid Centre, **www.smartgrids.no**