MEDIT

METHODS FOR ENERGY GRID ACTORS FOR PREVENTION, DETECTION AND REACTION AGAINST IT-FAILURES AND ATTACKS

The transformation in power generation comes along with an increased use of information and communication technology (ICT) at the distribution grid level. This poses new challenges for grid operation, especially in the area of IT security, as failures or interventions at the ICT level can have a direct and serious impact on secure grid operation. The increased integration of distributed energy resources and new consumers in the grid (e.g. electric vehicle charging infrastructure) increasingly leads to interactions between the participating energy grid actors and grid operation. Virtual power plant operators aggregate and control generation facilities, storage facilities and loads in the sense of a common electricity market and simultaneously provide system services required for network operation, such as balancing power.

In addition, due to the increased use of smart meters with control functions end customers have an increasingly active role within the energy market in both the private and commercial sectors.

Figure 1: MEDIT – Kick-Off-Meeting

The aim of the MEDIT research project is the development of technologies, concepts and methods for the detection, prevention and reaction against IT-attacks and failures for all energy grid actors in order to be able to guarantee a secure, stable and reliable supply in the German power system. In this context, future grid operation scenarios are defined and the future data traffic using ICT is analyzed. In order to investigate the interactions between ICT and energy systems and to develop innovative detection methods for IT attacks, an ICT energy co-simulation environment of both domains will be set up. In the course of the project, the Center for Grid Integration at RWTH Aachen University will be expanded in the field of ICT, in order to provide a realistic environment for the development of new IT security technologies. On this basis, new methods and technologies for ICT monitoring, application-oriented attack detection and reactive measures can be developed, validated and tested with regard to their applicability

for different energy grid actors. In addition, the impact of IT attacks and faults on the security of supply and stability of the electricity grid can be evaluated within this environment. Furthermore, demonstration tests for the realistic validation of the developed systems are carried out both in the laboratory and in the field. Based on the project results, recommendations for action can be derived for energy grid actors with regard to prevention, detection and reaction to IT attacks and failures with regard to their applicability. Subsequent open fields of action can be identified for future secure distribution grid operation.

The IFHT is responsible for the further development and integration of the power system simulation environment into the planned ICT Energy Co-Simulation. Subsequently, verification tests of the ICT energy co-simulation environment will take place at the Center for Grid Integration of RWTH Aachen University to verify the functionality and correctness of the mapping of real processes. The IFHT's analyses focus on the evaluation of the effects of IT attacks on energy network actors with regard to the stability of distribution networks. From this, measures can be derived to increase the resilience of distribution networks against disruptions caused by IT attacks.

Project information

Partners

- Fraunhofer FIT
- Fraunhofer FKIE
- Hochschule Bremen
- Schleswig-Holstein Netz AG
- devolo AG
- P3 Energy & Storage GmbH
- Kisters AG

Facts

- Acronym: MEDIT
- Duration: 10/2018 – 09/2021

Supported by:

Federal Ministry for Economic Affairs and Energy

on the basis of a decision by the German Bundestag

Contact

Philipp Linnartz
Research Associate
linnartz@ifht.rwth-aachen.de