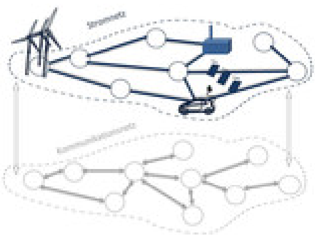
BINE Information Service
Energy research for application

Energy networks require comprehensive data communication in which security plays a key role. Bertikow substation in the Uckermark (Brandenburg)
© 50Hertz

Grid security 17.01.2018

Closing security loopholes in power grids

The way in which electricity distribution networks operate is changing considerably as a result of the energy transition. Decentralised systems are increasingly being connected via the Internet with the central control rooms of the energy providers for control purposes. The risks that can arise due to security loopholes in the information system are accordingly growing. In a guide, researchers at Bremen University of Applied Sciences show how the operational management can be secured and how the risks can be limited if measures fail.


The SEnCom project aims to reveal security- and reliability-relevant challenges in integrating communication infrastructure in the distribution networks.
© SEnCom

Traditional distribution networks transport electricity from centralised large-scale power plants via long-distance networks to the end consumers, such as industry, households and commerce. Today, the network design has to incorporate increasingly complex tasks. For example, the energy flow in the distribution network is reversed when wind energy and photovoltaic systems feed in decentrally. With new communication technology, power generators, loads and home storage systems are integrated so that they work in a grid-supportive manner. Last but not least, electromobility is now in the starting blocks.

That is why proprietary information processing systems without an Internet connection are a thing of the past. Standardised protocols are being established. Decentralised systems are connected to an energy supplier via a public communications network for control purposes. For this purpose, security functions need to be integrated into control systems, and traditional security measures from typical computer networks need to be adapted to the protocols and technical requirements of the new control systems. This is essential for ensuring that these can be used to secure process networks. Although grid operators are obliged to take measures to ensure a secure information and communication infrastructure in accordance with the German Energy Industry Act and the Federal Network Agency's IT security requirements catalogue, the potential attack scenarios and the risks to supply security are still largely unknown.

This is where the joint "System security of energy supply networks with integration of information and communication technologies" project, or SEnCom for short, comes into play. In the project, partners from business and research investigated the security- and reliability-relevant challenges in integrating communication infrastructure into the distribution networks. Here they analysed both the possibility of external interventions in the information and communication technology (ICT) systems as well as their impacts on the grid operation. The main focus of the investigations was on "attacks" on the ICT systems which could have an impact on the reliability of the supply and system stability of distribution grids as well as system-relevant repercussions for the interconnected grid.

The report from Bremen University of Applied Sciences is especially relevant for practice. It can be used as a guide for ensuring the security of distribution grids.
"The guide is intended to provide IT managers with support at energy suppliers and in particular for distribution grids. To this end, we have identified and summarised relevant standards with regard to information security in the German energy network, based on the IT security catalogue," says the head of the Computer Networks and Information Security research group, Professor Richard Sethmann, in summarising the goals.

"However, information security is not a one-off project," stresses Sethmann. "Despite all the efforts made, security loopholes can always occur as a result of human and technical errors. Information security must be an ongoing process."

The guide can be downloaded from the Bremen University of Applied Sciences website.

(me)