PRESS RELEASE

Ensuring security and reliability in smart meters

Close collaboration is key in fighting security issues

Today, GSGF published a report on the cyber security issues in smart meters and the associated advance metering infrastructure. While smart meters offer significant benefits, it is also understood that as software and communications become more pervasive, systems will become prone to previously alien issues – security being one of them. In this report, GSGF wants to highlight the fact that security and reliability cannot be isolated from each other.

It is expected that the global smart meter deployment will cross 800 million by 2020. Several geographies including North America and Europe have achieved a significant portion of their targets already. While utilities can realize substantial benefits from smart meters and associated platforms, GSGF's Cyber Security Work Group identified some concerns from a security standpoint, such as the risk of fraud or privacy concerns.

To begin with, there is a risk of widespread fraud if a security vulnerability is industrialized and manipulated meter readings can lead to substantial revenue loss for the utility. In addition, the presence of features such as over the air upgrades and a remote connect/disconnect switch can lead to a strategic vulnerability if an adversary is able to turn off power from millions of households. Last but not least there is also the issue of data collection: a smart meter directly interfaces with the end user and is perhaps the most important component in the smart grid eco-system from a privacy standpoint.

Moreover, there is no single uniform metering architecture that is followed globally. Countries have their unique requirements and the system is modeled to meet them, which makes it hard to ensure security. There are countries where the Distribution Network Operators own the meters, others where the suppliers own the meters and even others where the DNO's and the suppliers are one and the same. Such nuances will determine the roles and responsibilities of the stakeholders when it comes to security, according to the Work Group.

The network operators as well as the energy suppliers will have to conduct frequent Vulnerability/Threat/Risk assessments on their systems to ensure that they understand the system risks as it evolves and make sure appropriate mitigation actions are planned. Incident response and management is another area where it is critical to have pre-defined responsibilities for all stakeholders in a complex socio-technical system such as the power infrastructure.

In conclusion, the report indicates that it will require all involved parties—the equipment vendors, the network operators, the energy companies and the regulators coming together to ensure that security and reliability are treated together and that the proper target is the sum of the two, namely dependability.

PRESS RELEASE

Global Smart Grid Federation

The Global Smart Grid Federation (GSGF: http://www.globalsmartgridfederation.org/) is committed to creating smarter, cleaner electricity systems around the world. By linking the major public-private stakeholders and initiatives of participating countries, the federation shares best practices, identifies barriers and solutions, fosters innovation, and addresses key technical and policy issues. These and other activities help member organizations initiate changes to their country's electric systems to enhance security, increase flexibility, reduce emissions, and maintain affordability, reliability, and accessibility of electricity.

The Global Smart Grid Federation also works with the International Smart Grids Action Network (ISGAN: http://www.ieaisgan.org/) as well as with national and international policymakers to address the broad challenges of deploying smarter grids. This nexus provides bidirectional communication and collaboration, which envisions accelerated deployment of smart grids around the world and facilitates consensus-building within the international community to address concerns related to electricity systems and climate change.

More information

- GSGF: **www.globalsmartgridfederation.org**
- The working groups: **www.globalsmartgridfederation.org/about-gsgf/working-groups/**
- The members: **www.globalsmartgridfederation.org/members/**

Contact

Bieke Demaeghdt
Communication
EnergyVille
Thor Park Poort Genk 8300
3600 Genk
Belgium
T: +32 499 16 95 00
bieke.demaeghdt@energyville.be