AKE 10: Distributed Energy Generation, Electrical Grids

Time: Wednesday 11:30–12:15 Location: U A-Esch 1

Invited Talk AKE 10.1 Wed 11:30 U A-Esch 1

Wege zu einer sicheren und stabilen voll-regenerativen Elektrischen Energieversorgung — •Harald Weber — Universität Rostock, Institut für Elektrische Energietechnik

Im Zuge der Energiewende wird mehr und mehr elektrische Energie von Wind- und PV-Anlagen erzeugt. Diese Energie wird in großen chemischen Speichern gespeichert (Speicherkraftwerk). Diese neuen Player werden mit Umrichtern an das Drehstromnetz angeschlossen und weisen systembedingt keine Schwungmassen mehr auf. Die konventionellen Kraftwerke dagegen werden in ihrer Anzahl zurückgehen. Deshalb müssen die neuen Speicherkraftwerke alle Aufgaben der konventionellen Kraftwerke übernehmen. Das kann mit konventioneller Frequenzregelung oder aber mit neuartiger Winkelregelung geschehen.

AKE 10.2 Wed 12:00 U A-Esch 1

Modellbasiertes IT-Sicherheitssystem für vernetze Komponenten zukünftiger Energiesysteme — •Kathrin Reibelt, Ghada Elbez, Oliver Scherer, Jörg Matthes, Hubert B. Keller und Veit Hagenmeyer — IAI, KIT, Karlsruhe

Cyberangriffe und auch nachfolgend Schäden haben allgemein in den letzten Jahren immer stärker zugenommen. Dies ist auch darin begründet, dass vernetzte informationstechnische Systeme in immer zentraleren, kritischeren Bereichen zum Einsatz kommen. Im Bereich der kritischen Infrastrukturen birgt dies ein erhebliches Risiko. Die Energieversorgung ist inzwischen zum häufigsten Ziel von Cyber-Angriffen avanciert. Dabei zeigt die Vergangenheit, dass klassische IT-Sicherheitsmaßnahmen über eine Analyse des Kommunikationsverkehrs (Traffic) nur unzureichend Schutz bieten. Beispielsweise können Angriffe basierend auf False Data Injection kaum detektiert werden. Ein neuer Ansatz nutzt Modellinformationen über den physikalischen Teil des Systems aus, um die kommunizierten Messwerte zu verifizieren und zu validieren. Im Fall eines Angriffs lassen sich über verschiedene Verfahren korrumpierte Komponenten lokalisieren, was gezielte Gegenmaßnahmen erlaubt. Gezeigt werden insbesondere Fortschritte seit der letzten DPG-Tagung, auf der der grundlegende Ansatz vorgestellt wurde. Die auf statistischen Verfahren basierende Lokalisierung wird mit zusätzlichen Modellinformationen ausgewertet, was zu einer verbesserten Detektion von Angriffen führt.