AKE 13: Cyber Aspects in future Energy Systems

Time: Wednesday 16:00–16:45 Location: DÜL

Invited Talk AKE 13.1 Wed 16:00 DÜL

Digitale Herausforderungen für das Energiesystem der Zukunft — •Hubert Keller — Karlsruher Institut für Technologie, Institut für Automation und angewandte Informatik, Karlsruhe

Das Energiesystem der Zukunft besteht aus hoch verteilten und wechselwirkenden Komponenten, die sowohl Verbraucher als auch fluktuierende Erzeuger sind. Die Gesamtsystemstabilität wird nur durch eine umfassende Informations- und Kommunikationstechnologie unter Nutzung des Internets realisierbar sein. Damit sind die bisher hierarchisch und eher abgeschotteten Systemarchitekturen flach verteilt und gegenüber Dritten offen. Damit ist einerseits eine hohe Kommunikation erforderlich aber gleichzeitig auch die Gefahr von Cyber-Attacken erheblich gestiegen. Welche Gefahren in automatisierten Systemen und speziell im Energiesystem vorhanden sind, wie diese beherrschbar werden und welche Methoden hierfür einzusetzen sind wird am KIT intensiv erforscht. Sowohl das Reallabor Energy Lab 2.0 als auch die entsprechenden wissenschaftlichen Forschungsarbeiten zu Cyber-Security sind für die zuverlässige Funktion des zukünftigen Energiesystems unabdingbar. Nur durch eine neue Denkweise, Organisation und dem Einsatz zuverlässiger Softwaresysteme kann das Energiesystem abgesichert werden.

AKE 13.2 Wed 16:30 DÜL

Detektion und Lokalisierung von Cyber-Angriffen im Digitalisierten Energiesystem — •Kathrin Reibelt, Jörg Matthes, Hubert B. Keller und Veit Hagenmeyer — Institut für Automation und angewandte Informatik (IAI), Karlsruher Institut für Technologie (KIT), Karlsruhe

Cyberangriffe auf cyber-physikalische Systeme existieren bereits seit den Anfängen des Internets. Die informationstechnischen Gegenmaßnahmen werden im stetigen Wettlauf mit den Angriffsmethoden weiterentwickelt, wobei Angreifermodelle für zukünftige Cyberangriffe von begrenzten Fähigkeiten der Angreifer ausgehen. Im Zuge der Digitalisierung, die auch vor der kritischen Infrastruktur nicht Halt macht, ist dieses klassische Vorgehen nicht mehr ausreichend. Schäden durch erfolgreiche Angriffe können hier nicht einfach hingenommen werden und aufgrund der zunehmend professionelleren Akteure muss mit nahezu unbegrenzten Ressourcen der Angreifer gerechnet werden. Einfache, modellbasierte Gegenmaßnahmen begrenzen die Werte von Mess- und Stellgrößen auf definierte Intervalle. Diese klassischen Methoden versagen jedoch, wenn Angriffe im zulässigen Wertebereich bleiben und zulässige Kommandos nutzen. Das im Vortrag vorgestellte Verfahren berücksichtigt auch Abhängigkeiten der Größen durch die Nutzung eines physikalischen Anlagenmodells sowie Kenntnisse der informationstechnischen Eigenschaften der Komponenten. Es ermöglicht so die Detektion und Lokalisierung von Manipulationen sowie die Eingrenzung des Manipulationswegs. Die Verbesserung der Sicherheit für das jeweilige System kann mit ROC-Kurven objektiv eingeschätzt werden.