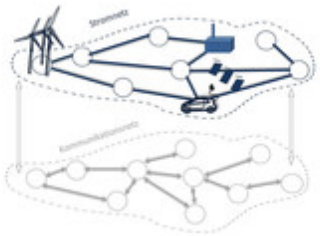
Energienetze benötigen eine umfassende Datenkommunikation, bei der Sicherheit eine zentrale Rolle spielt. Umspannwerk Bertikow in der Uckermark (Brandenburg)

Netzsicherheit 17.01.2018

Sicherheitslücken in Stromnetzen schließen



Das Projekt SEnCom untersucht die sicherheits- und zuverlässigkeitsrelevanten Herausforderungen bei der Integration einer Kommunikationsinfrastruktur in den Verteilungsnetzen.

Die Betriebsweise von Strom-Verteilnetzen ändert sich durch die Energiewende erheblich. Zunehmend arbeiten dezentrale Systeme über das Internet zur Steuerung mit zentralen Leitwarten der Energieversorger zusammen. Entsprechend wachsen die Gefahren, die durch Sicherheitslücken im Informationssystem auftreten können. In einem Leitfaden zeigen Forscher der Hochschule Bremen, wie sich die Betriebsführung absichern lässt und wie der Schaden begrenzt werden kann, wenn die Maßnahmen doch versagen.

Klassische Verteilnetze transportieren Strom von zentralen Großkraftwerken über Fernnetze zu den Endverbrauchern, wie Industrie, Haushalte und Gewerbe. Heute kommen auf die Netzgestaltung komplexere Aufgaben zu. So kehrt sich beispielsweise im Verteilnetz der Energiefluss um, wenn Windenergie- und Photovoltaikanlagen dezentral einspeisen. Mit neuer Kommunikationstechnik sind Stromerzeuger, Verbraucher und Heimspeicher so eingebunden, dass sie netzdienlich arbeiten. Nicht zuletzt steht die Elektromobilität in den Startlöchern.

Deshalb gehören proprietäre informationsverarbeitende Systeme ohne Internetverbindung der Vergangenheit an. Es etablieren sich standardisierte Protokolle. Dezentrale Systeme werden über ein öffentliches Kommunikationsnetz zur Steuerung mit einem Energieversorger verbunden. Hierfür müssen Sicherheitsfunktionen in Steuerungssysteme integriert und traditionelle Sicherheitsmaßnahmen aus den typischen Computernetzen auf die Protokolle und technischen Anforderungen der neuen Steuerungssysteme adaptiert werden. Das ist die Voraussetzung, damit sie zur Absicherung von Prozessnetzen eingesetzt werden können. Wenngleich Netzbetreiber nach dem Energiewirtschaftsgesetz sowie dem Sicherheitskatalog der Bundesnetzagentur zu Maßnahmen für eine sichere Informations- und Kommunikations-Infrastruktur verpflichtet werden, sind die potenziellen Angriffsszenarien sowie die Risiken hinsichtlich der Versorgungssicherheit noch weitestgehend unbekannt.

Hier setzt das Verbundprojekt „Systemsicherheit von Energieversorgungsnetzen bei Einbindung von Informations- und Kommunikationstechnologien“, kurz SEnCom an. Projektpartner aus Wirtschaft und Forschung untersuchten die sicherheits- und zuverlässigkeitsrelevanten Herausforderungen bei der Integration einer

Kommunikationsinfrastruktur in die Verteilungsnetze. Dabei analysierten sie sowohl die Möglichkeit externer Eingriffe in die Informations- und Kommunikationstechnik (IKT) als auch deren Auswirkungen auf den Netzbetrieb. Im Fokus der Untersuchungen standen vor allem „Angriffe“ auf die IKT, die Auswirkungen auf die Versorgungszuverlässigkeit und Systemstabilität von Verteilungsnetzen sowie systemrelevante Rückwirkungen auf das Verbundnetz haben können.

Eine besondere Praxisrelevanz hat der Bericht der Hochschule Bremen. Er kann als Leitfaden für die Sicherheit von Verteilnetzen verwendet werden.

„Der Leitfaden soll IT-Verantwortlichen bei Energieversorgern und insbesondere für Verteilungsnetze eine Hilfestellung bieten. Hierzu haben wir relevante Standards mit Bezug auf die Informationssicherheit im deutschen Energienetz, ausgehend von dem IT-Sicherheitskatalog, identifiziert und zusammengefasst“, fasst der Leiter der Forschungsgruppe Rechnernetze und Informationssicherheit Prof. Dr. Richard Sethmann die Ziele zusammen.

„Informationssicherheit ist aber kein einmaliges Projekt“, betont Sethmann. „Durch menschliche und technische Fehler können trotz aller Bemühungen immer Sicherheitslücken auftreten. Informationssicherheit muss ein andauernder Prozess sein.“

Der Leitfaden kann auf der Website der Hochschule Bremen heruntergeladen werden.

(me)