Anomalieerkennung in Energienetzen

Motivation

Die Erweiterung von Stromnetzen durch Informations- und Kommunikationstechnologie zum sogenannten Energieinformationsnetz (bzw. Smart Grid) ist Voraussetzung für die Sicherung der Versorgungs- und Netzstabilität bei der vermehrten Nutzung verteilter, alternativer Energiequellen. Die durchgängige Kommunikationsvernetzung und das Einbeziehen vieler verteilter Einspeisepunkte erhöht die Anfälligkeit des Energienetzes gegenüber IT-Störungen, z.B. durch Fehlkonfigurationen oder Ausfälle und gegenüber ungerichteten oder gezielten IT-Angriffen. Durch die enge Kopplung zwischen Energie- und Informationsnetz wirken sich Beeinträchtigungen des Informationsnetzes unmittelbar auf die Zuverlässigkeit und Sicherheit der Energieversorgung aus.

Ziele

Ziel des Projektes ist die Erkennung und Abwehr von nicht bestimmungsgemäßen Eingriffen in operative Steuerung und Organisation des Energieversorgungsnetzes durch Mittel der Informationstechnologie. Dies umfasst insbesondere folgende Teilziele:

1. Erkennen von absichtlichen, zielgerichteten und unbefugten Eingriffen auf Kommunikationsverbindungen und Einrichtungen der industriellen Informationstechnologie im Energieversorgungsnetz. Solche Eingriffe mit kriminellem oder gar terroristischem Hintergrund stellen nicht nur eine schwerwiegende Bedrohung für die Verfügbarkeit der Energieversorgung dar, sondern könnten durch Außerkraftsetzen von Sicherheitseinrichtungen auch Menschenleben und Sachwerte unmittelbar bedrohen.

2. Erkennen von unabsichtlichen Einwirkungen auf jene Kommunikationsverbindungen und Einrichtungen durch Schadsoftware (Viren, Trojaner). Diese Einwirkungen können als „Kollateralschäden“ solcher Schadsoftware betrachtet werden. Diese beeinträchtigen vorrangig die Verfügbarkeit der Energieversorgung, aber auch weitergehende Auswirkungen sind vorstellbar.

3. Erkennen von unabsichtlichen Einwirkungen auf jene Kommunikationsverbindungen und Einrichtungen durch Ausfälle von Komponenten sowie durch Software- oder Konfigurationsfehler.

4. Abwehr der genannten Einwirkungen durch präventive Maßnahmen, insbesondere Härtung der Kommunikationsverbindungen und Einrichtungen der industriellen Informationstechnologie im Energienetz sowie erhöhter Verteidigungsmaßnahmen zum Schutz eines Kernbetriebs, mit dem die Energieversorgung gesichert werden kann.

5. Abwehr der genannten Einwirkungen durch geeignete reaktive Maßnahmen nach deren Er-kennung, z.B. Isolation der des Einfallstors, Eindämmung des Krisenherdes, Herbeiführen eines besonders gehärteten Notbetriebs, Initiierung eines Krisenmanagements durch die Anlagenbetreiber.

Eckdaten

Kurztitel

SmartDefense

Forschungsschwerpunkt

Digital Technologies

Laufzeit

01.01.2015 - 31.12.2019

Fördergeber

Ziele

- Erkennen von absichtlichen, zielgerichteten und unbefugten Eingriffen
- Erkennen von unabsichtlichen Einwirkungen
- Abwehr durch präventive Maßnahmen
- Abwehr durch geeignete reaktive Maßnahmen nach deren Erkennung

Bundesministerium für Wirtschaft, Landesentwicklung und Energie

Projektleitung

Prof. Dr.-Ing. Peter Fröhlich