EnergyNetworkSec

Ausfallssicherheit digitalisierter Verteilungsnetze für elektrische Energie

Programm / Ausschreibung	KIRAS, Kooperative F&E-Projekte, KIRAS Kooperative F&E-Projekte 2017	**Status**	abgeschlossen
Projektstart	01.11.2018	**Projektende**	30.04.2021
Zeitraum	2018 - 2021	**Projektlaufzeit**	30 Monate
Keywords			

Projektbeschreibung

Durch die zunehmende Digitalisierung der Netze für die Verteilung elektrischer Energie erhöht sich die Anfälligkeit dieses Systems für Cyber-Attacken beträchtlich. Um die Ausfallssicherheit dieser kritischen Infrastruktur zu gewährleisten, ist ein wirksamer Schutz vor Angriffen unbedingt erforderlich. Derzeit existierende Sicherheitsmaßnahmen beschränken sich vor allem auf die Absicherung des Zugangs zu diesen Systemen. Im Sinne der „Security in Depth“ müssen allerdings unbedingt zusätzliche Maßnahmen getroffen werden, um auch nach einem möglichen Überwinden der Zugangskontrollen den Angriff erkennen und adäquate Reaktionen setzen zu können. Dies kann durch eine laufende Überwachung des Netzwerkverkehrs innerhalb des Systems erfolgen, durch die Abweichungen vom Normalverhalten des Automatisierungssystems – Anomalien – festgestellt werden können. Derzeit gibt es keine derartigen Überwachungssysteme, die speziell auf die Erfordernisse der IT-Architekturen von Energieverteilungsnetzen ausgerichtet sind.
Ziel des Projekts EnergyNetworkSec ist die Erforschung von Möglichkeiten zur Anomalie-Erkennung in Automatisierungsnetzen der Energieverteilung. Dazu müssen Muster des Normalverhaltens des Systems formal modelliert werden, um im laufenden Betrieb das Systemverhalten mit diesen Mustern vergleichen zu können und gegebenenfalls einen Alarm auslösen zu können. Im Gegensatz zu herkömmlichen statistischen Methoden der Mustererkennung sollen in diesem Projekt Verfahren der syntaktischen Mustererkennung erforscht werden. Dabei wird das Normalverhalten mit Hilfe einer formalen Grammatik modelliert und die laufende Überprüfung wird dann mit Hilfe eines Algorithmus durchgeführt, der die Korrektheit des Netzwerkverkehrs an Hand der Grammatik prüft. Auf Grund der besonderen Eigenschaften eines Automatisierungssystems – relativ repetitives Verhalten über die Zeit – scheint eine solche Vorgangsweise vielversprechend zu sein. Dieser Ansatz wurde bislang noch nicht verfolgt und würde daher eine interessante Innovation darstellen.
Bei Erkennung einer Anomalie im Netzwerkverkehr des Systems muss diese klassifiziert werden, um gegebenenfalls geeignete Gegenmaßnahmen auswählen und setzen zu können. Dazu können Methoden aus der Theorie der formalen Sprachen und insbesondere auch der Übersetzung und begleitenden Fehlererkennung herangezogen werden. Das Projekt umfasst auch eine Proof-of-Concept Implementierung des Überwachungssystems
Auf Grund der bereits eingeleiteten Automatisierung und Digitalisierung der Verteilungs-systeme für elektrische Energie (unter anderem durch die großflächige Ausrollung von Smartmeter Infrastrukturen) besteht dringender Forschungsbedarf in diesem Bereich.

Abstract

The progressively increasing automation and digitization of distribution networks for electrical energy opens up a big new range of possibilities for cyber-attacks. In order to guarantee the resilience of such critical infrastructures the implementation of effective protection mechanisms is essential. Security measures generally used today are limited to access control methods. State of the art security, however, demands “security in depth”: additional measures must be implemented that become effective if an attacker has succeeded in overcoming the access barriers. Among others this can be realized by monitoring the network traffic with the goal of detecting anomalies in the system’s behaviour. As of today such monitoring systems suitable for IT architectures of distribution systems for electrical energy do not exist.
The main objective of the project EnergyNetworkSec is researching technologies for anomaly detection in automation networks of energy distribution systems. To this end a formal model of normal system behaviour must be developed. The monitoring process uses this model to detect anomalies and set appropriate actions. Unlike conventional pattern matching methods based on statistics this project will focus on syntactic pattern matching: the normal behaviour of the system is modelled by a formal grammar and the monitoring process uses parsing algorithms to check the network traffic for compliance with the grammar. Due to the specific properties of an industrial automation system – which generally shows a highly repetitive behaviour – such an approach seems promising. So far this has not been pursued and therefore would be a substantial innovation.
When detected an anomaly in the network traffic must be classified with respect to its cause in order to decide the necessary actions. For this, too, methods from the theory of formal languages and especially from compiling and error handling can be adapted. The project includes a proof-of-concept implementation of the monitoring system.
Because of the fact that automation and digitization of distribution systems for electrical energy is already in full process – as for example the extensive roll-out of smart metering infrastructures – there is an urgent need of research in this area.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten Forschungs GmbH

Projektpartner

- Wels Strom GmbH
- nic.at GmbH
- RadarServices Smart IT-Security GmbH
- Hochschule für Angewandte Wissenschaften St. Pölten GmbH