Fraunhofer
IPK

FRAUNHOFER-INSTITUT FÜR PRODUKTIONSANLAGEN UND KONSTRUKTIONSTECHNIK IPK

1 *Verteilte Energieversorgung stellt neue Herausforderungen an die sichere Kommunikation.*

IT-SICHERHEIT FÜR SICHERHEITSKRITISCHE ENERGIE-INFRASTRUKTUREN

Fraunhofer-Institut für Produktionsanlagen und Konstruktionstechnik IPK
Pascalstr. 8–9
10587 Berlin

Ansprechpartner
Max Klein
Geschäftsfeld Automatisierungstechnik
Telefon: +49 30 39006-466
max.klein@ipk.fraunhofer.de

Laufzeit
01.09.2018 – 31.08.2020

Projektpartner
AUCOTEAM GmbH, PI Informatik GmbH

www.ipk.fraunhofer.de

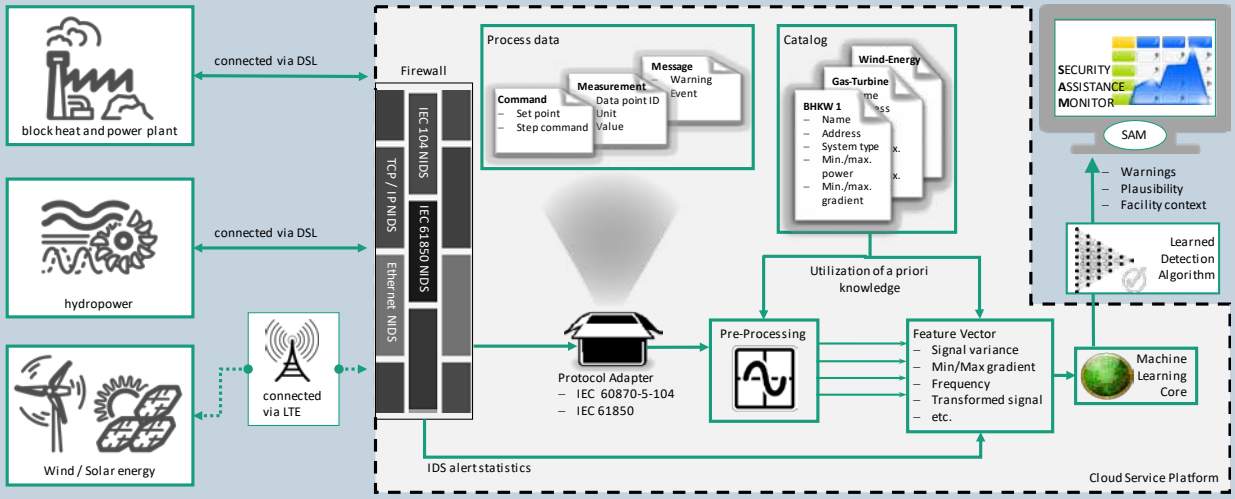
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

IT-Sicherheitsüberwachung in der Energiewende

Die Energiewende bildet eine wesentliche Herausforderung des 21. Jahrhunderts, nicht zuletzt sind hierbei die deutsche und europäische Forschungslandschaft gefordert. Die konkreten Ziele sind in der Hightech-Strategie der Bundesregierung beschrieben. Ein aufkommender Trend ist die Nutzung von erneuerbaren Energien aus vielfältigen, dezentral arbeitenden Erzeugern. Dies wirft neue Fragestellungen hinsichtlich sicherer Kommunikation zwischen allen Beteiligten auf. Mit dem Projekt Reaktive IT-Sicherheitsüberwachung automatisierter technischer Anlagen in sicherheitskritischen Energie-Infrastrukturen (EnerSec) im Zuge der Ausschreibung »KMU-innovativ: Informations- und Kommunikationstechnologie (IKT)« zielen wir auf eine sichere Integration dezentral arbeitender Erzeuger in die vorhandene Leittechnik.

Vernetzte Energieversorgung

Viele dezentrale Stromerzeuger, wie Windkraftwerke, Biomasseanlagen oder Blockheizkraftwerke (BHKW) liefern Energie für das Stromnetz und müssen dies mit zentralen Leitstellen koordinieren. Weil verschiedene Energiequellen zeitlich verschieden verfügbar sind, muss die Deckung der Grundlast durch Echtzeitregelung mit ständigem Prozessdatenaustausch abgestimmt werden. Dieses Energie-Management erfolgt über »virtuelle Kraftwerke«, wie sie vom Projektpartner Aucoteam GmbH vertrieben werden. Da es für den Datenaustausch nur selten eigene Kommunikationsleitungen gibt, wie im Falle großer Kraftwerke, erfolgt der Austausch der Fernwirkprotokolle (IEC 61850 oder IEC 60870-5-104) meist über herkömmliche Internet- oder Funkverbindungen. Hierdurch ergibt sich das Risiko der Verfälschung dynamischer Anlageninformationen. Angreifer könnten die Einspeisung unbemerkt manipulieren oder



die Anlagen beschädigen, was Einfluss auf die Netzstabilität haben kann.

Reaktive Sicherheit

Unsere Zielsetzung besteht in der Erschließung eines neuartigen technischen Ansatzes zur Erhöhung der Sicherheit für Stromversorger bzw. Stromnetze durch »Reaktive IT-Sicherheitsüberwachung« automatisierter technischer Anlagen. Reaktive Verfahren gehen im Moment des Angriffs auf diesen ein und grenzen sich damit ab von präventiven Vorgehensweisen wie Verschlüsselung und Zugriffsbeschränkung, welche im Vorfeld die Fremdeinwirkung erschweren. Die angestrebte Lösung soll die konkreten Inhalte der Nutzdaten berücksichtigen und das jeweilige Domänenwissen einbinden können.

Mit Künstlicher Intelligenz Angriffe erkennen

Ausgangspunkt der Angriffserkennung sind lokale Komponenten zur Erfassung und schnellen Auswertung von Daten vor Ort bzw. an kritischen Punkten der IT-Kommunikation, die rückwirkungsfrei den Datenaustausch überwachen. Die in Echtzeit mitlaufende Auswertung läuft über regelmäßig aktualisierte Detektionsmodelle und zentrale Auswertungskomponenten als Services in einer Cloud-Plattform. Der Cloud-Ansatz ermöglicht hierbei einen permanenten Abgleich von Angriffsmustern über alle Systeme verschiedener Standorte und stets aktuelle Analyseprogramme, die als Service aufgerufen werden. Die Expertise für Cloud-basierte Lösungen der Firma PI-Informatik ermöglicht hier eine schnelle Umsetzung der Verfahren. Die überwachten Prozessdaten beinhalten unter anderem Signale für Leistung und Frequenz, aber auch auftretende Events. Mit dem fachlichen Hintergrundwissen werden charakteristische Eigenschaften in einem Feature-Vektor zusammengetragen und können dann Machine-Learning-Algorithmen übergeben werden. Die betrachteten Signale werden hinsichtlich markanter Merkmale im Vorfeld ausgewertet, was dem Lernverfahren erleichtert, bedeutsame Änderungen in den entsprechenden Größen zu erkennen.

Von der Idee zur praktischen Erprobung

Die aufgezeigte Problemstellung für virtuelle Kraftwerke mit ihren verteilten Einspeisestationen ist repräsentativ für eine Entwicklung hin zu dezentralem Management der Energieversorgung. Um die im Forschungsprojekt adressierten Verfahren auch auf reale Szenarien zu übertragen, entsteht ein Demonstrator. Referenzobjekt dieser FuE-Aktivitäten ist ein Energie-Pool (virtuelles Kraftwerk), bestehend aus informationstechnischem Steuerungssystem und mehreren automatischen Klein-Energieerzeugern. Zunächst sollen physikalische Simulationen aller beteiligten Komponenten in einem Testbed zusammengebracht werden. Darüber hinaus müssen, unabhängig von der Erforschung von Detektionsverfahren, entsprechende Angriffsvektoren generiert werden. Ein Demonstrator soll reale Steuerungstechnik und exemplarische Simulationsmodule bereitstellen, woran verschiedene Detektionsalgorithmen verglichen werden können.

2 *Aus den Prozessdaten lernen KI-Verfahren, normalen Betrieb und Anomalien zu unterscheiden.*