KI-basierte Erkennung und resiliente Vermeidung von Cyber-Angriffen und technischen Störungen bei virtuellen Kraftwerken und dezentralen Energieanlagen

Abschlussbericht zum Teilvorhaben:

Iterative Feldtests und Integration eines Störfallinformationssystem für virtuelle Kraftwerke

Förderkennzeichen 03EI4028E
Förderzeitraum 01.04 2021 – 31.03.2024
Autor: Lars Siebert

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Ansprechpartner:
Lars Siebert
ENERTRAG SE
Gut Dauerthal 3
17291 Schenkenberg
lars.siebert@enertrag.com

I. Kurze Darstellung

Fortschreitende Digitalisierung und Vernetzung bietet im Bereich der erneuerbaren Energien viele Vorteile, macht aber auch angreifbar. Während traditionelle Energieversorgungssysteme in erster Linie durch konventionelle IT-Schwachstellen bedroht sind, eröffnen die neuen digitalen Infrastrukturen Angreifern die Möglichkeit, gezielte und oft komplexe Angriffe auf dezentrale Energieanlagen, die als virtuelle Kraftwerke zusammengefasst werden, durchzuführen. Dieses Teilvorhaben hatte die Testung und Implementierung mit realen Daten zum Ziel, die in anderen Teilprojekten entwickelten Verfahren zur Ausfallerkennung und zur Abwehr von Cyberangriffen unter realistischen Bedingungen zu testen, um deren Effektivität und Zuverlässigkeit zu gewährleisten. Ziel war es, durch diese praxisnahen Tests wertvolle Erkenntnisse zu gewinnen, die zur weiteren Optimierung und Verfeinerung der Sicherheitsmechanismen im Bereich der erneuerbaren Energien beitragen werden.

Zusammen weisen die Konsortialpartner umfassende Kenntnisse und praktische Erfahrungen in den Bereichen der erneuerbaren Energien und der IT-Sicherheit auf. Das IT-Sicherheitsgesetz 2.0 stellt eine wesentliche Weiterentwicklung der bisherigen gesetzlichen Vorgaben dar und legt erweiterte Anforderungen und Standards für die IT-Sicherheit fest.

Das Gesamtprojekt , bestehend aus insgesamt sieben Arbeitspaketen, hat den Aufbau eines umfassenden Störfallinformationssystems (SIS) zur automatischen Erkennung von Störungen und Cyberangriffen mittels fortschrittlicher, KI-basierter Technologien sowie eine resiliente Reaktion auf solche Vorfälle, um umgehend geeignete Maßnahmen zur Abwehr und Minderung der Auswirkungen zu initiieren, zum Gesamtziel.

Wind- und Photovoltaikparks sind teilweise auf Funkverbindungen basierenden Technologien wie GSM (G2), GPRS und UMTS (G3) an das Kommunikationsnetz angeschlossen, da sie sich größtenteils außerhalb von Ballungsräumen befinden. Zum Teil erfolgt die Anbindung auch über leitungsgebundene Techniken wie DSL oder LWL. Zum Datenaustausch werden unterschiedlichste Protokolle und Datenmodelle wie IEC61850, OPC(-XML)DA, MODBUS und auch proprietäre Protokolle verwendet. Weiterhin werden verschiedene Techniken wie VPN, HTTPS und IPSec eingesetzt, um die Informationssicherheit zu gewährleisten. Daraus ergibt sich eine Vielzahl von Möglichkeiten für die Etablierung von Sensoren für die Angriffserkennungssysteme, die jeweils ihre Vor- und Nachteile hinsichtlich Geschwindigkeit, Sicherheit und Verfügbarkeit

haben. Die Anzahl von Cyberangriffen auf Rechnernetzwerke und Computersysteme ist in den letzten Jahren dramatisch angestiegen. Die Verwendung marktüblicher Sicherheitssysteme wie einer Firewall als alleiniger Schutz gegen Cyberangriffe wird in Zukunft, aufgrund immer zielgerichteter und professionellerer Angriffe auf die IKT-Infrastruktur, nicht mehr ausreichen. Erst eine Kombination verschiedener Komponenten, wie beispielsweise einer Firewall in Verbindung mit einem Intrusion Detection System (IDS) und Intrusion Prevention System (IPS), das den gesamten Netzwerkverkehr auf ungewöhnliche Aktivitäten überwachen kann, ermöglicht eine sichere und frühzeitige Erkennung und Vermeidung des Cyberangriffs. Je eher ein Einbruchsversuch erkannt und erfolgreich abgewehrt werden kann, desto geringer ist der daraus entstehende Schaden. Zum Sicherheitskonzept heutiger IT-Infrastruktur von Unternehmen gehören daher immer häufiger IDS/IPS- als proaktiven Schutz gegen Cyber-Angriffe.

Es handelt sich hierbei um Kooperationsprojekt zwischen den sechs Partner:

- ANE GMBH & CO. KG
- DECOIT GmbH
- ENERTRAG SE
- Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik IEE
- Fraunhofer-Institut für Sichere Informationstechnologie SIT
- Hochschule Hannover

Außerdem wurde mit SECUINFRA GmbH ein externer Partner für die Wartung und den langfristigen Betrieb eines Störfallinformationsystemes als strategischer Partner ausgewählt.

II. Eingehende Darstellung

a. Für welche Ziele wurde die Zuwendung verwendet inkl. Gegenüberstellung mit den Zielen

Ziel des Projekts war die Entwicklung und Erprobung von Systemen, Verfahren und Methoden zur automatisierten Erkennung und Vermeidung von Angriffen auf dezentrale Energieanlagen und Anlagenpools, wie virtuellen Kraftwerken. Dabei standen die Besonderheiten des Energiesystems als kritische Infrastruktur im Fokus der Untersuchungen. Dazu wurden drei Teilziele definiert und bearbeitet:

1) Entwicklung sowie Anpassung von Verfahren und Methoden zur Erkennung und Vermeidung von Cyber-Angriffen auf dezentrale Energieanlagen und virtuelle Kraftwerke während des Betriebes sowie Integration dieser Verfahren in IDS/IPSSysteme

Auf energiewirtschaftliche Standards und Kommunikationstechnologien angepasste Verfahren und Systeme zur Angriffserkennung und Angriffsvermeidung werden benötigt, um auch in Zukunft die Sicherheit gegen die steigende Anzahl von IT-Angriffen auf den Energiesektor zu gewährleisten. Aufgrund von großen Datenmengen bei der Kommunikation mit den angeschlossenen Energieanlagen und dem virtuellen Kraftwerk sind Verfahren und Methoden notwendig, die diese Datenmenge effizient – insbesondere auch in bestehenden Systemen - verarbeiten und dennoch Cyberangriffe erkennen sowie vermeiden können.

2) Schaffung einer realitätsnahen Plattform zur Verfahrens- und Methodenentwicklung für die IDS/IPS-Systeme mit Hinblick auf das Verhalten der Anlagen

Eine realitätsnahe Plattform zur Verfahrensentwicklung wird benötigt, damit das IDS/IPS-System und die darin verwendeten Verfahren auf das spätere Einsatzgebiet hin optimiert werden können. Dabei ist es notwendig den Normalzustand realitätsnah abzubilden, um eine Anomalie im Verhalten sowie besonderes Verhaltensmuster überhaupt detektieren zu können. Dabei wurde insbesondere darauf geachtet, dass der Normalzustand der betrachteten Systeme abgebildet werden kann, um das Training von Anomalie-basierten Verfahren bestmöglich zu unterstützen. Die Entwicklung weiterer Verfahren, wie zum Beispiel Signatur- oder Spezifikations-basiert, sollte durch diese Plattform ebenso ermöglicht werden.

3) Nachweis der Effektivität der entwickelten Verfahren durch Feldtests mit realen Anlagen und virtuellen Kraftwerken

Die Leistungsfähigkeit des IDS/IPS-Systems sollte mit Hilfe eines Feldtests nachgewiesen werden. Dafür wurde das entwickelte IDS/IPS-System aufgebaut, die entwickelten Verfahren integriert. Für die Evaluation der Verfahren sollten mögliche IT-Angriffe auf die Anlagen bzw. Anlagenpools simuliert werden.

Trotz der Verzögerungen bei der Bereitstellung und Anbindung der Testdaten durch personelle Veränderungen und der Tatsache, dass Testdaten aufgrund der technischen Abstimmungen im Bereich des SIS verzögert wurden und der Export von Daten für das Projekt durch technische Barrieren eingeschränkt war, konnte das Projekt seine Hauptziele erreichen.

Als Betreiber von dezentraler Energie-Infrastruktur und Anbieter von spezialisierter Software für die Betriebsführung von erneuerbaren Energieanlagen (EE-Anlagen) spielte unser Unternehmen eine entscheidende Rolle im Projekt für iterative Feldtests. Wir waren in der Lage, eine umfassende Sammlung von Protokolldaten aus verschiedenen relevanten Quellen bereitzustellen, um die Anforderungen des Projekts zu erfüllen und wertvolle Einblicke zu gewinnen.

Die Protokolldaten stammten aus einer Vielzahl von Quellen innerhalb unserer IT- und Energieinfrastruktur. Dazu gehörten detaillierte Daten von Servern, die als zentrale Komponenten für die Verarbeitung und Speicherung von Informationen fungieren, sowie Daten aus der Netzwerkinfrastruktur, die für die Kommunikation und Datenübertragung zwischen den verschiedenen Systemen und Geräten verantwortlich ist. Darüber hinaus wurden auch spezifische Anlagendaten, die den Betrieb und den Zustand der Energieanlagen erfassen, in die Sammlung integriert. Diese umfassenden Datensätze umfassten sowohl Betriebsdaten als auch sicherheitsrelevante Informationen, die für die Durchführung der Feldtests von grundlegender Bedeutung waren.

Die gesammelten Daten wurden sorgfältig aus den verschiedenen Systemen extrahiert, aggregiert und dem Projektteam zur Verfügung gestellt. Dieser erste Schritt der Datensammlung bildete die Grundlage für die nachfolgenden Schritte im

Rahmen der Feldtests. Durch die Bereitstellung dieser umfassenden und vielfältigen Datensätze konnte das Projektteam sicherstellen, dass die Tests auf einer soliden und repräsentativen Datenbasis durchgeführt werden konnten.

Im nächsten Schritt wurde ein detailliertes und realistisches Testszenario aufgebaut, das es ermöglichte, die entwickelten Verfahren zur Anomalieerkennung unter praxisnahen Bedingungen zu erproben. Das Szenario wurde so konzipiert, dass es die komplexen und dynamischen Bedingungen widerspiegelt, die in einer realen Betriebsumgebung auftreten können. Hierdurch konnten die entwickelten Anomalieerkennungsverfahren auf ihre Effektivität und Zuverlässigkeit getestet werden.

Zur Unterstützung der Feldtests wurde ein Störfallinformationssystem eingerichtet, das kontinuierlich sowohl die Energieanlagen als auch die Netzwerkinfrastruktur überwacht. Dieses System ist darauf ausgelegt, alle relevanten Betriebs- und Sicherheitsdaten in Echtzeit zu überwachen und kontinuierlich auf Auffälligkeiten zu analysieren. Es wurde so konzipiert, dass es automatisch mögliche Anomalien oder Störungen identifiziert und entsprechende Warnmeldungen ausgibt. Durch diese permanente Überwachung konnte das Projektteam die Anomalieerkennung auf ihre Praxistauglichkeit überprüfen.

Insgesamt trug unsere umfassende Datenbereitstellung und die sorgfältige Konzeption des Testszenarios wesentlich dazu bei, die Ziele des Projekts erfolgreich zu erreichen. Die gewonnenen Erkenntnisse aus den Feldtests ermöglichten es, die entwickelten Sicherheits- und Überwachungslösungen weiter zu verfeinern und zu optimieren, um eine höhere Zuverlässigkeit und Effektivität in der Überwachung und Sicherstellung der Betriebssicherheit der dezentralen Energie-Infrastruktur zu gewährleisten.

b. Wichtigste Positionen des zahlenmäßigen Nachweises

Alle während der Projektarbeit verwendeten Mittel (82.000,96 €) wurden für die Zahlung von Gehältern (Personalkosten) verwendet. Geplante Mittel für die Abschreibung von Ausrüstungen wurden nicht verwendet.

c. Notwendigkeit & Angemessenheit der geleisteten Arbeiten

Die Arbeiten innerhalb des Projektes wurden ausschließlich durch ENERTRAG-interne Ressourcen abgedeckt und führten zu den erwarteten Ergebnissen. Arbeiten in den Arbeitspaketen AP0 sowie AP6 wurden erfolgreich durchgeführt und ermöglichten das Erreichen der gesetzten Ziele.

AP0 Projektkoordination

- Teilnahme an AP-Leiter-Meetings (genereller Status)
- Teilnahme an Konsortialtreffen
- Interne und externe Koordination und Berichterstattung

AP 6 Iterative Feldtests

1. Bereitstellung von Betriebsdaten:

Das Projekt benötigt in den anderen AP diese Daten, um Verfahren zur Angriffserkennung zu entwickeln.

2. Bereitstellung von OT-Infrastrukturdaten

Für eine bessere Anomalieerkennung wurden zusätzlich zu den Anlagendaten Protokolle auf der OT-Infrastruktur dem Projekt zur Verfügung gestellt.

3. Integration des SIS aus AP4

Die von DECOIT GmbH entwickelte SIS-Lösung „Scanbox" wurde gemäß deren Vorgaben in unserem OT Netzwerk eingerichtet.

4. Aufbau eines Testszenarios für die anderen Arbeitspakete

In dem finalen SIS wurde eine Testumgebung für die anderen Projektteilnehmer geschaffen.

d. Voraussichtlicher Nutzen & Verwertbarkeit der Ergebnisse

Die entwickelten Technologien und Innovationen können in einem breiten Anwendungsspektrum eingesetzt werden. Die Digitalisierung der Energiewirtschaft, die Integration verteilter Erzeuger und die wachsende Bedeutung von Resilienz und Cybersicherheit in kritischen Infrastrukturen schaffen eine hohe Nachfrage nach den im Rahmen des Projekts entwickelten Lösungen. Diese Technologien bieten sowohl funktionale als auch wirtschaftliche Vorteile gegenüber bestehenden Konkurrenzlösungen und eröffnen bedeutende Verwertungsmöglichkeiten für verschiedene Anwendergruppen, insbesondere am Standort Deutschland. Die im Projekt entwickelten Verfahren zur

Anomalieerkennung bieten gegenüber bestehenden Konkurrenzlösungen erhebliche Vorteile in Bezug auf die Systemzuverlässigkeit und Resilienz. Diese Lösungen ermöglichen es Netzbetreibern, potenzielle Störungen frühzeitig zu erkennen und präventive Maßnahmen zu ergreifen, wodurch Ausfallzeiten und Betriebsmittelschäden minimiert werden können.

Außerdem bieten die Erkenntnisse dieses Projektes vielfältige Erweiterungsmöglichkeiten, die sowohl im wissenschaftlichen als auch im wirtschaftlichen Kontext weiterverfolgt werden können. Besonders die fortschreitende Digitalisierung der Energiewirtschaft, die Notwendigkeit zur Erhöhung der Resilienz in kritischen Infrastrukturen sowie die weitergehende Integration erneuerbarer Energien schaffen Potenzial für zukünftige Innovationen und Forschungsarbeiten.

Ein zentraler wissenschaftlicher Anschlussbereich ist die Weiterentwicklung der Algorithmen zur Anomalieerkennung und Fehlerbehebung in Energiesystemen. In einer nächsten Phase könnten diese Algorithmen durch den Einsatz von Künstlicher Intelligenz (KI) und Maschinellem Lernen weiter optimiert werden, um noch präzisere und schnellere Reaktionen auf ungewöhnliche Systemverhalten zu ermöglichen. Dies könnte die Grundlage für zukünftige Forschungsvorhaben in den Bereichen KI-basierte Energiesysteme und Selbstheilung von Energienetzen darstellen.

Die zunehmende Abhängigkeit von IKT in der Energiewirtschaft erfordert kontinuierliche Weiterentwicklungen im Bereich der Cybersicherheit. Hier besteht ein großer Forschungsbedarf, insbesondere in der Sicherung von dezentralen und dynamischen Netzwerken, die in zukünftigen Energiesystemen eine wesentliche Rolle spielen.

e. Bekannt gewordene technische Fortschritte auf dem Gebiet bei anderen Stellen

Solche Fortschritte sind uns nicht bekannt.

f. Erfolgte/geplante Veröffentlichung nach Nr. 11

Im Rahmen dieses Projektes erfolgten und erfolgen von ENERTRAG SE keine Veröffentlichungen von Ergebnissen.