

Sachbericht zum Verwendungsnachweis

Vorhabenbezeichnung: **Verbundprojekt WAIKIKI**

„Wissensbasierte Anomalieerkennung mittels Künstlicher Intelligenz in Kritischen Infrastrukturen“

Teilvorhaben:

Demonstratorentwicklung und Anwendungskordinator für Großanlagen der Energieerzeugung

BMBF-Programm:

IT-Sicherheit - Selbstbestimmt und sicher in der digitalen Welt

Förderkennzeichen: 16KIS1203

Laufzeit des Vorhabens: 01.09.2020 – 31.08.2023

Verlängerung: 01.09.2023 – 31.08.2024

Berichtszeitraum: 01.09.2020– 31.08.2024

Inhaltsverzeichnis

1. Projektverlauf und Ergebnisse	3
1.1 Allgemeines	3
1.1.1 Ursprüngliche Aufgabenstellung	3
1.1.2 Kooperation im Projekt	3
1.1.3 Wesentliche Ergebnisse	3
1.2 Gewinnung eines Praxispartners	4
1.3 Infrastruktur	4
1.3.1 Allgemeiner Aufbau	4
1.3.2 Die Computing Plattform	5
1.3.3 Entwicklung von mobilen Sensoren	6
1.3.4 Experimentierplattform	7
1.3.5 Integration der Systeme	9
1.4 Datenfluss	9
1.4.1 Datenfluss für Netzwerkdatenanomalienerkennung	9
1.4.2 Datenfluss für Kontextdatenanomalienerkennung	10
1.4.3 Ausgabe	11
1.5 Visualisierung der Ergebnisse im Splunk.....	12
1.5.1 Modul Netzwerkanomalien	12
1.5.2 Modul Kontextanomalien	12
1.5.3 Modul Netzwerk- und Kontextanomalien	12
1.5.4 Darstellung der Positionierung des Förderers	13
1.5.5 Darstellung der Lichtintensität	14
1.5.6 Darstellung der Kontextdaten der Positionierung und Lichtintensität	15
1.5.7 Darstellung der Anomalienerkennung mittels Splunk	15
1.6 Verwertbarkeit der Ergebnisse und voraussichtlicher Nutzen	16
2. Vergleich des Vorhabenstands mit der ursprünglichen Planung.....	18
3. Die wichtigsten Positionen des zahlenmäßigen Nachweises	19
4. Die Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten.	20
5. Der während der Durchführung des Vorhabens dem ZE bekannt gewordene Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen	21
6. Die erfolgten oder geplanten Veröffentlichungen der Ergebnisse	22

1. Projektverlauf und Ergebnisse

1.1 Allgemeines

1.1.1 Ursprüngliche Aufgabenstellung

Zukunftsfähige Sicherheitslösungen müssen für eine hohe Anzahl von Technologien geeignet sein und die dezentrale Organisation des Energienetzes berücksichtigen. Daher sollen im Vorhaben WAIKIKI Algorithmen des Deep Learning (die vielfältige und komplexe Netzdaten abbilden können) geschickt mit klassischen maschinellen Lernverfahren (die üblicherweise in Lerneffizienz und Analyseperformanz überlegen sind) kombiniert werden, um die Vorteile beider Ansätze optimal auszunutzen. Zudem soll eine Graph-basierte Visualisierung für eine nutzerverständliche Darstellung der trainierten Modelle und Anomalien geschaffen werden und so eine intelligente netzbasierte und nachvollziehbare Anomalieerkennung für Energienetze entstehen.

Ziele sind dabei,

- die Erklärbarkeit der Ergebnisse für die Anwender (Netzbetreiber) herzustellen,
- das effektive Lernen vielfältiger und komplexer Netzkommunikation auf Basis weniger oder unvollständiger Trainingsdaten zu ermöglichen und
- die bisherigen Fehlerraten von selbstlernender Anomalieerkennung auf diesem Gebiet signifikant zu senken.

Die Entwicklung der angestrebten Methoden erfolgt auf Basis realer Daten aus Infrastrukturen von neuer und konventioneller Energieerzeugung sowie höchst modernen Energienetzen (Smart Grids).

1.1.2 Kooperation im Projekt

Mit folgenden wissenschaftlichen Einrichtungen wurde im Rahmen des Projektes kooperiert:

- Brandenburgische Technische Universität Cottbus-Senftenberg (BTU), Lehrstuhl IT-Sicherheit
- Technische Universität Chemnitz, Lehrstuhl Künstliche Intelligenz

Des Weiteren erfolgte die Zusammenarbeit nachfolgend aufgeführten industriellen Partnern:

- ASCORI GmbH, Cottbus
- Migosens GmbH, Mühlheim a. d. R.
- [REDACTED]

1.1.3 Wesentliche Ergebnisse

Im Rahmen der Arbeitspakete wurden zunächst die Anforderungen an ein KI-basiertes Anomalie-Erkennungssystem erarbeitet sowie die Nutzerakzeptanzkriterien definiert. Anschließend erfolgte die Planung der zwei benötigten Plattformen, der

- Experimentierplattform,
- Computing Plattform sowie

die Planung der

- Integration der Experimentierplattform bei ASCORI und
- Integration der Computing Plattform [REDACTED] der LEAG.

Nach dem Abschluss der Planungsarbeiten wurden die notwendigen Hardwareteile beschafft, die jeweiligen Plattformen montiert, in ihren geplanten Umgebungen integriert und in Betrieb genommen.

Nachfolgend konnten das Sammeln und Verarbeiten der Sensor- und Kontextdaten sowie das Training der Modelle beginnen.

Die Verarbeitung sowie die Bewertung der Daten starteten nach der Bereitstellung der jeweiligen KI-Modelle durch die BTU-Cottbus-Senftenberg sowie durch die TU-Chemnitz. Parallel begann bereits die Entwicklung des Demonstrators inklusive der notwendigen Auswertungen zur Bewertung der Ergebnisse. Die regelmäßige Evaluation der Ergebnisse aus den KI-Modellen erforderte immer wieder Anpassungsarbeiten am Demonstrator und deren Auswertungen. Diese Arbeiten dauerten bis zum Projektende 08/2024 und auch etwas darüber hinaus an.

1.2 Gewinnung eines Praxispartners

Für das Projekt konnte unser Kunde LEAG als Projekt- und Praxispartner gewonnen werden. Folgende Zielstellungen waren damit verbunden:

- Mitschnitt und Analyse der Daten im Leittechnik- und Steuerungsnetz sowie im [REDACTED]
- Rückwirkungsfreie Gewinnung realer Daten aus der Praxis
- Bau des Prototyps im produktionstechnischen Umfeld
- Platzierung der Analyseeinheiten innerhalb eines Prozessleitsystems, Expertensystem und das Prozessnahe Datennetz
- Überwachung der Netzgrenze/Firewall („Prozess-Engineering“) in Richtung externe Netze sowie Punkten mit größtem Risiko mit größerem Anteil Standard-IT
- Einrichtung eines exemplarischen Systems auf der Ebene „Prozessautomatisierung“

1.3 Infrastruktur

1.3.1 Allgemeiner Aufbau

Gemeinsam mit den Projektpartnern wurde entschieden zur Auswertung der Daten zwei unterschiedliche Plattformen aufzubauen:

- eine Computing Plattform sowie
- eine Experimentierplattform.

Über die Computing Plattform (CPF) kann sich ein benannter Personenkreis der Konsortialpartner einwählen und auf den, ihnen zugewiesenen, VMs anmelden, arbeiten sowie auf gemeinsam geteilte Ressourcen zurückgreifen. Zu diesen Ressourcen gehört u.a. der Fileserver, auf dem die Netzwerkmitschnitte, und Extraktionen von diesen, abgelegt sind. Die KI-Module der Universitäten können von dem Fileserver Daten einlesen, verarbeiten und Ergebnisse herauschreiben. Splunk ist dabei die Präsentationsebene, auf welchem die Ergebnisse dargestellt werden.

Um unabhängig der LEAG und Versuchsgenehmigungen kurzfristig Netzwerk- und Kontextinformationen zu generieren, mitzuschneiden und auszuwerten, ist die Experimentierplattform (EXPF) geschaffen worden. Diese erlaubt auch „Angriffe“ gegen die Plattform zu führen und damit in den Aufzeichnungen Anomalien zu erzeugen. Die autarke Experimentierplattform ist über ein VPN mit der Computing Plattform angebunden. Damit können automatisiert die Informationen von der EXPF zur CPF transportiert und gespeichert werden.

Zur Erfassung der Netzwerkdaten wurden kleine MiniPCs (Sensoren) mit mehreren Netzwerkinterfaces installiert.

Nachfolgende Grafik beschreibt den allgemeinen Aufbau:

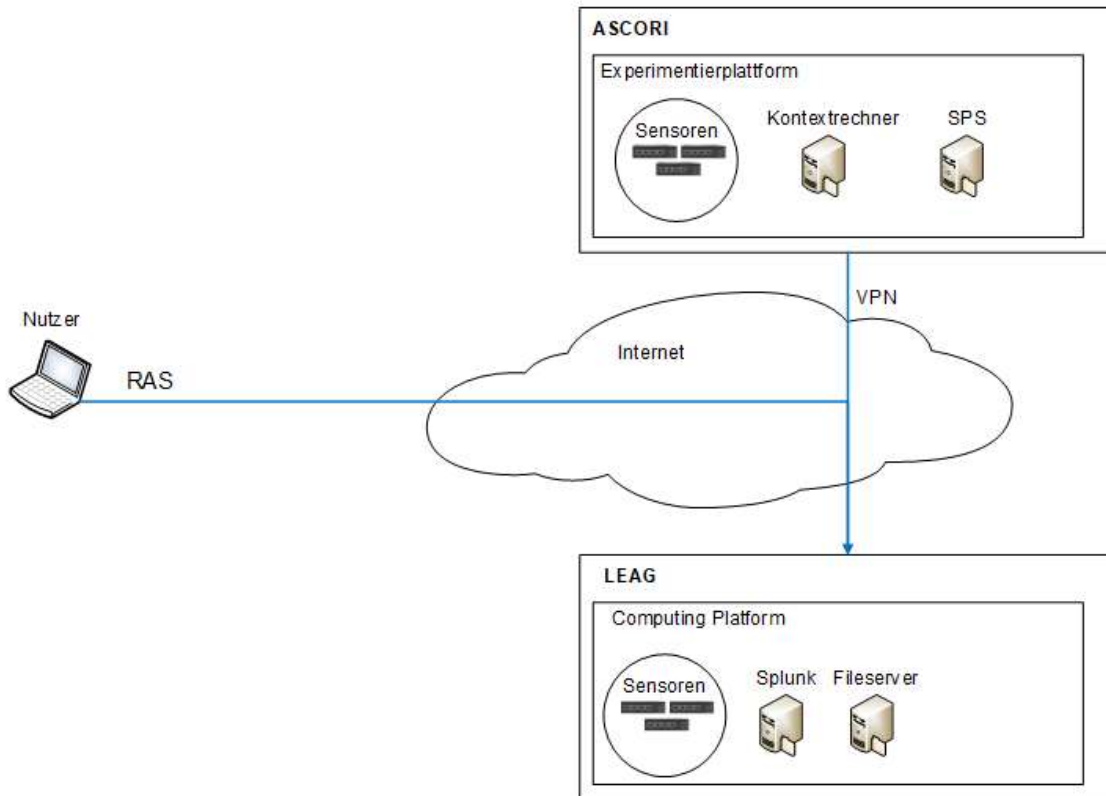


Abbildung 1 Allgemeines Kommunikationsschema zum Projekt

1.3.2 Die Computing Plattform

Verwendungszweck

Um die großen anlaufenden Datenmengen zu speichern und zu verarbeiten, spielt die CPF eine signifikante Rolle. Hier laufen alle wesentlichen Informationen zusammen. Unter anderem erfolgt auf den Virtuellen Maschinen (VMs) der CPF das Training der KI-Systeme. Sie benötigen die auf dem zentralen Fileserver abgelegten Daten. Des Weiteren erfolgt hier die Untersuchung der Prozessdaten auf Anomalien.

Lokalisierung

Die IT-Infrastruktur der Computing Plattform ist in der LEAG am Standort [REDACTED] mit räumlicher Nähe zu den Zielsystemen aufgebaut. Dies erlaubt kurze Übertragungswege der Netzwerk- sowie Logdaten von der LEAG internen Infrastruktur zur WAIKIKI Plattform.

Aufbau

Die IT-Infrastruktur des Demonstrators beinhaltet die notwendige Hardware und System-Software, die sicher in bestehende industrielle Umgebungen integriert werden kann, Datenschnittstellen bereitstellt und die Ausführung der WAIKIKI-Softwarealgorithmen gewährleistet. Während die Sensoren die Netzwerkmitschnitte auf dem Fileserver ablegen, verbindet sich ein Server einmal am Tag mit einem durch die LEAG bereitgestellten Fileserver, auf dem die Kontextdaten abgelegt sind und kopiert diese auf den Fileserver der CPF.

Wesentliche Hardware-Bestandteile sind eine Firewall, ein Layer 2 Switch, ein Layer 3 Switch, einen HyperVisor, ein SAN und ein NAS. Netzwerkkomponenten wie Firewalls und Switches sind Cisco Geräte. HyperVisor und SAN sind von Fujitsu, das NAS ist von Synology.

Die **Firewall** bildet die Sicherheitskomponente zwischen der CPF und dem Internet sowie als Einwahlpunkt für Nutzer der Konsortialpartner und als VPN-Endpunkt zwischen CPF und EXPF. An dem **Layer 2 Switch** sind alle Hardwarekomponenten und Netze angeschlossen.

Der **Layer 3 Switch** bildet dabei die routende Instanz.

Das **Storage Area Network (SAN)** stellt den Speicherbereich für den HyperVisor zur Verfügung und der **HyperVisor** die notwendigen Ressourcen für die VMs.

Das **NAS** dient zur Datensicherung und -wiederherstellung.

Services

Neben der Infrastruktur werden einige Software-Services benötigt, die für die Sicherstellung der Gesamtfunktion des Systems zentral zur Verfügung stehen müssen.

Dazu gehören folgende Services:

- **Monitoring** Werkzeug zur Überwachung der VMs in Bezug auf Performance (Software Icinga).
- **Remote Access Service (RAS)** für die Einwahl der Nutzer, um mit der CPF arbeiten zu können, und als Site-2-Site Endpunkt (Cisco AnyConnect).
- **Fileservice** als gemeinsame Datenablage, auf dem Netzwerk- und Kontextdaten zur Laufzeit geschrieben und von den VMs gelesen und verarbeitet werden (NFS).
- **Reporting Plattform** zum Darstellen der verarbeiteten Daten (Software Splunk).

1.3.3 Entwicklung von mobilen Sensoren

Allgemeine Aufgaben des Sensors

Die permanente und automatisierte Erfassung von prozessgesteuerten Daten für die WAIKIKI Anomalie-Erkennung ist ein weiterer, notwendiger Baustein. Dazu sind Daten-Kollektorsysteme erforderlich, die an verschiedene, auch räumlich abgesetzte Datenquellen anzuschließen sind. Die Daten-Kollektorsysteme bestehen aus Hardware- und Software-Komponenten. Sie müssen die Daten aus den produktiven Anlagen rückwirkungsfrei abgreifen und dem WAIKIKI-System vollständig zur Verfügung stellen. Die Rückwirkungsfreiheit ist mittels SPAN-Port realisiert. Ein SPAN-Port übermittelt dabei den Netzwerkverkehr ausschließlich unidirektional an den Sensor. Der Sensor kann über diesen Port weder mit anderen Netzwerkteilnehmern noch dem Switch selbst kommunizieren.

Nachfolgende Grafiken zeigen die wesentlichen Sensorkomponenten:



Abbildung 2 Sensor



Abbildung 3 Festplatte

Lokalisierung

Die örtliche Unterbringung der Sensoren änderte sich während des Projektverlaufes. Während diese zunächst an den Zielsystemen direkt platziert wurden mit einer 8 TB externen Festplatte als Datenspeicher, sind sie final zentral an der CPF angeschlossen worden und konnten somit direkt auf den Fileserver schreiben. Die externen Festplatten an den Sensoren wurden bei dieser Anordnung nicht mehr benötigt.

Aufbau

Der Sensor ist ein passiv-gekühlter lüfterloser Mini PC mit vier Netzwerk-, einem USB- und diversen Monitoranschlüssen, was Vorteile in staubigen Industrieanlagen mit sich bringt.

Die Netzwerkanschlüsse dienen folgenden Aufgaben:

- Management-Port,
- SPAN-Interface (auf diesem Port erhält der Sensor vom Switch die Netzwerkmitschnitte)
- OUT-Interface, welches die Daten an den Fileserver schickt.

Services

Der Sensor kann mittels extern angeschlossener USB-Festplatte Daten lokal schreiben oder diese über das Netzwerk an einen Fileserver über das NFS-Protokoll transferieren. Die Daten werden in ein PCAP-File geschrieben. Das erfolgt solange, bis entweder eine 100 MB Dateigröße oder die Zeitgrenze von 5 Minuten erreicht wurden. Danach wird ein neues File geöffnet. Des Weiteren prüft er die Verfügbarkeit seines Speichers und setzt das Schreiben fort, falls die Verbindung verloren gegangen sein sollte. Zu Analyse Zwecken kann der Sensor die IP-Header Pakete extrahieren und an Splunk direkt schicken.

Systemauswahl

Hardware-seitig besteht der Sensor aus einem kleinem lüfterlosen Mini PC. In ihm sind 4 GB RAM und eine 128 GB SSD verbaut. Softwareseitig wurde als Betriebssystem das ressourcenschonende Rocky Linux gewählt. Der AntiVirus Schutz von ESET prüft den Sensor auf Virenfreiheit. Mit Chrony synchronisiert der Sensor seine Systemzeit mit einem Zeitserver. TCPDump erfasst die ankommenden Netzwerkdaten. Das Python Script steuert dabei TCPDump, die Header Extraktion und das Übertragen der Daten sowie gegebenenfalls selbstverwaltete Neustarts einzelner Software-Komponenten im Fehlerfall.

1.3.4 Experimentierplattform

Allgemeine Aufgaben der Experimentierplattform

Die EXPF soll dabei ein vereinfachtes Modell einer Industrieanlage darstellen. Dies erlaubt unabhängig von einer Produktivumgebung „Angriffe“ über das Netzwerk gegen diese zu starten. Dies wäre bei der LEAG nicht möglich gewesen. Der Sensor erhält die Netzwerkdaten und der Kontextrechner die Loginformationen (Kontextdaten).

Durch die ZEDAS Mitarbeiter wurde u.a. einer der drei Sensoren (siehe Abbildung 5 - roter Rahmen unten links) angeschlossen und umkonfiguriert, sowie der Kontextrechner (roter Rahmen oben) angepasst.

Nachfolgende Grafik zeigt den allgemeinen Aufbau der Kommunikationsinfrastruktur der Experimentierplattform.

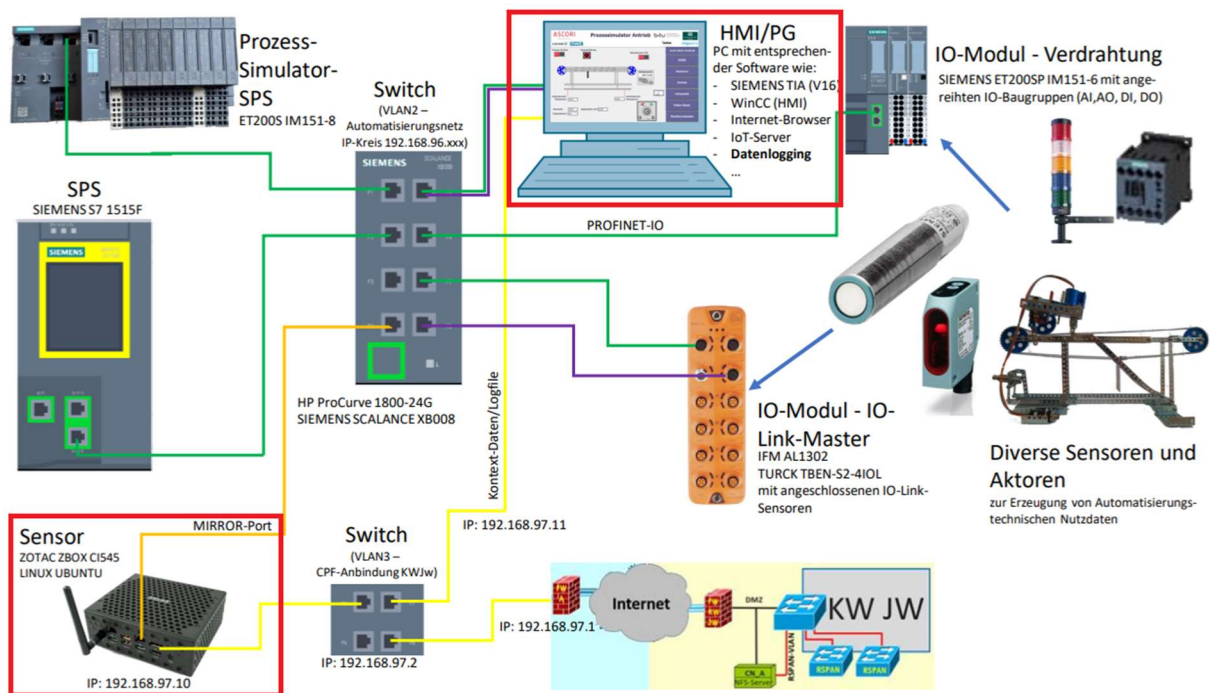


Abbildung 4 Kommunikationsinfrastruktur der Experimentierplattform

Lokalisierung

Die EXPf ist in Cottbus beim Konsortialpartner ASCORI aufgebaut.

Aufbau

Eine tiefgehende Beschreibung des Aufbaus ist in dem Abschlussbericht ASCORIs enthalten. Durch die Kombination aus diversen Sensoren und Aktuatoren und deren Steuerung erlaubt die EXPf das Erzeugen von Netzwerk- und Kontextdaten. Durch den modifizierten Sensor ist es ASCORI möglich gewesen die Datenerfassung eigenständig zu starten. Dabei werden die Daten über ein VPN-Tunnel von der EXPf zur CPF übertragen.

Services

Durch die Integration des Sensors und die transparente Anbindung der beiden Plattformen kann zu jedem beliebigen Zeitpunkt ein Messversuch auf Knopfdruck gestartet und beendet werden.

1.3.5 Integration der Systeme

Die beiden Plattformen mussten zur Erfüllung ihrer Aufgaben miteinander verbunden werden.

Die Sensoren integrieren sich sowohl in die EXPF (siehe Abbildung 5) als auch CPF (siehe Abbildung 6) mit minimalem Konfigurationsaufwand auf Seiten der Sensoren. Die IP-Adressen der Sensor-Netzwerk-Interfaces werden ihrer Umgebung angepasst und der Fileshare entsprechend der Umgebung geändert.

Da die EXPF transparent mit einem Site-to-Site VPN angebunden ist, bricht die Übertragung mangels Internet-/Tunnel Stabilität vom Sensor Richtung Fileshare der CPF regelmäßig ab. Dadurch wurde der Kontextrechner der EXPF als temporärer Zwischenspeicher/Fileshare verwendet, der kontinuierlich Daten zum Fileshare der CPF verschiebt. Dies hat eine Anpassung des Sensors im Einsatz auf der EXPF zur Folge, indem der Zielpfad zum Schreiben der Netzwerkdaten geändert werden muss.

Durch die Integration der Sensoren in die EXPF können Messungen von ASCORI per Knopfdruck des Steuerungssystems eigenständig durchgeführt werden. Da die EXPF an die CPF angebunden ist, werden alle notwendigen Informationen an derselben Stelle zusammengeführt.

Über die Ferneinwahl auf die CPF können Messungen innerhalb der LEAG gestartet werden, ohne dass ein Mitarbeiter vor Ort fahren muss (siehe Abbildung 1 Allgemeines Kommunikationsschema zum Projekt).

1.4 Datenfluss

1.4.1 Datenfluss für Netzwerkdatenanomalienerkennung

Zum Beginn des Messstartes werden alle Sensoren für die automatische Aufzeichnung aktiviert. Diese schreiben Netzwerkmitschnitte im PCAP-Format und kopieren diese auf den Fileserver. Zeitgleich werden aus den PCAP-Daten die Header-Informationen extrahiert, auf dem File-Server abgelegt und an Splunk geschickt. In der Trainingsphase liest die AI die erhaltenen Daten vom Fileserver und generiert ihr Modell. In der Detektionsphase schreibt die AI eine Detektionsdatei auf den Fileserver entsprechend in einem Ordner dem Ursprungssystem zugehörig (██████████).

Die Netzwerkmitschnitte wurden zu jeder Zeit aufgehoben, um gegebenenfalls neu zu trainieren oder eventuelle Fehler auf Basis der Rohdaten zu prüfen.

1.4.2 Datenfluss für Kontextdatenanomalienerkennung

Der Datenfluss der Kontextdaten unterscheidet sich zum Datenfluss der Netzwerkdaten, da die Sensoren hier keine Rolle spielen. Die Kontextdaten werden von den LEAG-Servern exportiert und auf einem Fileserver im Internet bereitgestellt. Um diese Informationen zu erlangen und auf den Fileserver der CPF zu speichern, verbindet sich der Server eBIS1 (external Business Integration Server) auf der CPF mit dem Fileserver der LEAG über [REDACTED] [REDACTED] einmal am Tag. Die erlangten Daten werden dann auf dem Fileserver analog zu den Netzwerkdaten in die entsprechenden Ordner kopiert. Die KI greift auf diese Daten zu und wird mit diesen trainiert oder detektiert Anomalien - je nach Phase. In der Detektionsphase wird auch hier eine Detektionsdatei geschrieben.

1.4.3 Ausgabe

Insgesamt entstehen drei Detektionsdateien. Die beiden zuvor erstellten Detektionsdateien werden eingelesen und damit der Zusammenhang zwischen Netzwerk- und Kontextdaten hergestellt. Der hergestellte Zusammenhang wird erneut in eine finale Detektionsdatei geschrieben. Die zwei Detektionsdateien für Kontext- und Netzwerkdaten und die finale Detektionsdatei werden dann zur Visualisierung an Splunk geschickt, wie in nachfolgender Grafik dargestellt.

Analog zu den Kontext- und Netzwerkdaten findet ebenfalls eine Aggregation der übermittelten Daten statt.

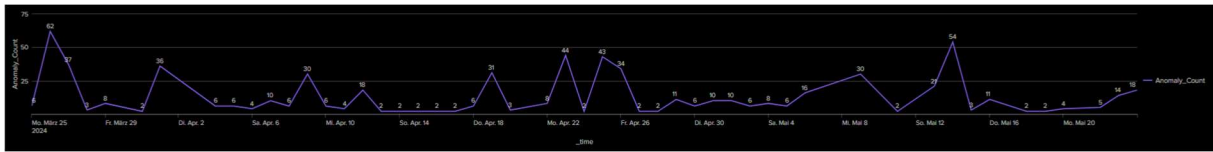


Abbildung 7 CPF - Visualisierung Splunk Anomaliezusammenhang (aggregiert)

1.5.4 Darstellung der Positionierung des Förderers

Zu den von der EXPF erfassten und in Splunk angezeigten Daten gehören die Positionierung des Förderers. Eingezeichnet ist die obere und untere Systemgrenze. Innerhalb dieser Grenze kann/sollte sich der Förderer bewegen. Vom System wird ihm dabei ein Zielwert vorgegeben, zu welchem er sich bewegen soll. Der Wert bezieht sich auf die Entfernung zum Sensor. Die Grafik zeigt den gemessenen Wert.



Abbildung 8 EXPF – position of the conveyor

1.5.5 Darstellung der Lichtintensität

Zusätzlich ist die EXPF mit einem Lichtsensor ausgestattet. Zu sehen sind drei Messzeiträume. Zwischen den Messzeiträumen wurde interpoliert (Auffüllung der Daten). Dies ist erkennbar an den geraden Anstiegen.

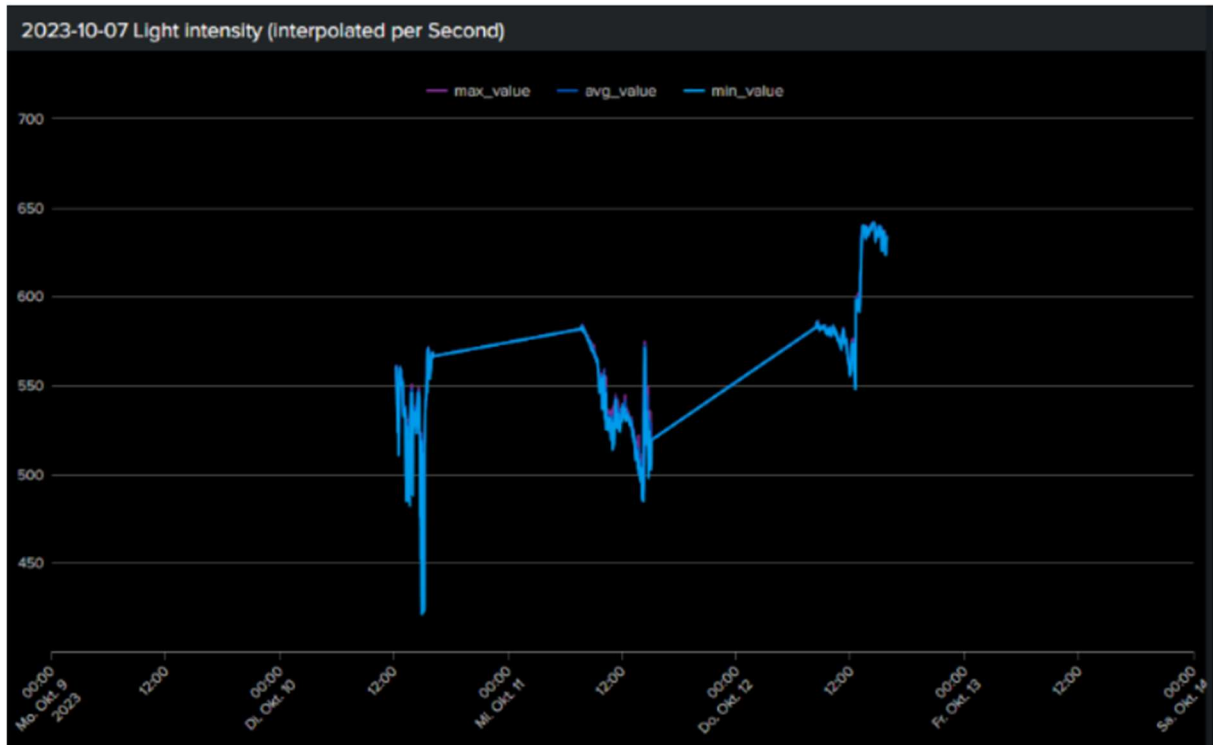


Abbildung 9 EXPF – light intensity

1.5.6 Darstellung der Kontextdaten der Positionierung und Lichtintensität

Die geschriebenen Kontextdaten der EXPF wurden ebenfalls in Splunk eingelesen und visualisiert. Dazu wurden die Messwerte des Positionierungsantriebes und des Lichtsensors sind aus den Logdaten extrahiert.

2023-10-07 Pre-processed logged context and key value as raw data

Select logging module: All X Select system: All

_time	domain	module	system	act_value	target_value	log_message
2023-10-10 12:13:33.542	waikiki.expf.kontext	Operation	001MA_001-M1			RUNTIME START - Initializing....
2023-10-10 12:13:35.854	waikiki.expf.kontext	Operation	001MA_001-M1		5800	Positionierantrieb Wartezeit geändert (ms)
2023-10-10 12:13:35.882	waikiki.expf.kontext	Process	001MA_001-M1		5800	Positionierantrieb Wartezeit geändert (ms)
2023-10-10 12:13:35.185	waikiki.expf.kontext	Operation	001MA_001-M1		100	Positionierantrieb Untere Grenzposition geändert
2023-10-10 12:13:35.117	waikiki.expf.kontext	Process	001MA_001-M1		100	Positionierantrieb Untere Grenzposition geändert
2023-10-10 12:13:35.132	waikiki.expf.kontext	Error	001AN.001			Nothalt quittiert/gegangen
2023-10-10 12:13:35.148	waikiki.expf.kontext	Process	001AN.001			Prozessbetrieb wegen Nothalt gestoppt
2023-10-10 12:13:35.168	waikiki.expf.kontext	Operation	001AN.001			Nothalt quittiert/gegangen
2023-10-10 12:13:35.562	waikiki.expf.kontext	Process	002LIGHT_-R1	561.67		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:36.562	waikiki.expf.kontext	Process	002LIGHT_-R1	561.58		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:37.558	waikiki.expf.kontext	Process	002LIGHT_-R1	561.53		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:38.562	waikiki.expf.kontext	Process	002LIGHT_-R1	561.42		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:39.511	waikiki.expf.kontext	Process	002LIGHT_-R1	561.47		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:40.507	waikiki.expf.kontext	Process	002LIGHT_-R1	561.4		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:41.507	waikiki.expf.kontext	Process	002LIGHT_-R1	561.35		Beleuchtungsstaerkesensor aktueller Messwert in Ohm
2023-10-10 12:13:43.607	waikiki.expf.kontext	Process	002LIGHT_-R1	561.28		Beleuchtungsstaerkesensor aktueller Messwert in Ohm

Abbildung 10 EXPF – Kontextdaten Positionierung und Lichtintensität

1.5.7 Darstellung der Anomalieerkennung mittels Splunk

Splunk bietet selbst eine integrierte Funktion zur Anomalieerkennung. Diese kann auf Eindimensionalen Messreihen angewendet werden – dies trifft hier zu. In Abbildung 21 sind zwei Anomalien erkannt worden. Diese wurden rechts im Messverlauf gelb und punktuell eingezeichnet.

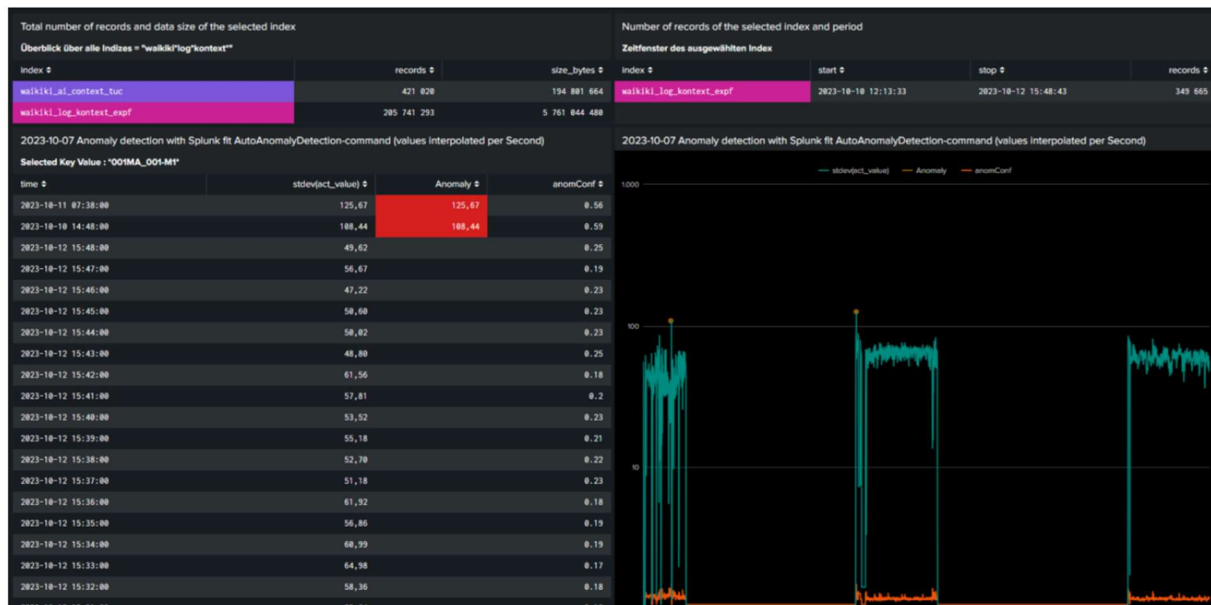


Abbildung 11 EXPF – Anomalieerkennung mit Splunk

1.6 Verwertbarkeit der Ergebnisse und voraussichtlicher Nutzen

Mit nachfolgend aufgeführten Punkten können die Ergebnisse des Projektes zusammengefasst und bewertet werden:

- **Rückwirkungsfreiheit**
 - Die Verfahren und Technologien wurden erfolgreich getestet und zeigten laut Aussagen der LEAG keine Rückwirkungen auf die zu überwachenden Leitsysteme.
- **Erkennungsrate und Fehlalarmrate**
 - **Erkennungsrate (RPR):** Die Erkennungsgenauigkeit zeigte gute bis sehr gute Ergebnisse, jedoch wurden nur synthetische Angriffsmuster verwendet. Eine weitere Bewertung mit realen Angriffsmustern ist notwendig.
 - **Fehlalarmrate (FPR):** Es wurden signifikante Fortschritte erzielt, die Fehlalarmrate konnte deutlich reduziert werden. Dennoch sind weitere Verbesserungen erforderlich und möglich, zum Beispiel durch die weitere Einbeziehung von Kontextinformationen, um letztendlich die Nutzerakzeptanz zu erhöhen.

Genauere Angaben zu Erkennungs- und Fehlalarmraten sind den Berichten und Veröffentlichungen der BTU Cottbus-Senftenberg sowie der TU Chemnitz zu entnehmen.
- **Demonstrator**
 - Der Technologiedemonstrator wird als gelungen und im Rahmen des Projektziels als vollkommen ausreichend bewertet. Natürlich hat der Demonstrator keine Produktreife und ein dauerhafter Einsatz in der Produktion ist in diesem Entwicklungsstand nicht möglich. Das gehörte aber auch nicht zu den Zielen dieses Projektes. In Folgeprojekten müsste entsprechender Aufwand in die Software und das Nutzerinterface gesteckt werden, um das Nutzerinterface einfacher, die Software insgesamt sicherer und die Ergebnisübersichten nachvollziehbarer zu gestalten.
- **Bedienung und Wartung**
 - Die Einfachheit in Betrieb und Wartung wurde in dem Projekt nicht ausreichend adressiert und bedarf weiterer Forschung bzw. weiteren Aufwandes. So ist es u.a. wichtig, dass die entwickelten Lösungen mit geplanten Änderungen in den Zielsystemen umgehen können. Eine gute Nutzerakzeptanz erfordert selbstlernende Prozeduren für technische Änderungen. Des Weiteren müssen die verwendeten KI-Methoden sowie die daraus resultierenden Ergebnisse nachvollziehbar und erklärbar sein.

Insgesamt kann man das Projekt als erfolgreich betrachten. Das wird sowohl von der ZEDAS-GmbH als auch von den beteiligten Projektpartnern so eingeschätzt. Die eigentlichen Ziele wurden erreicht. Eine Produkt- und Marktreife zu erzielen, gehörte nicht zu den Projektzielen. Es bedarf erheblicher Aufwendungen in die Entwicklung einer Software, die in robusten Produktionsumgebungen einsetzbar ist.

Verwertung der Ergebnisse

Die ZEDAS-GmbH ist weiterhin mit ihren Produkten zedas@asset und zedas@cargo in der Bahnbranche, speziell in den Bereichen Bahnlogistik, Infrastrukturinstandhaltung sowie Flotteninstandhaltung unterwegs. Zu den Kunden gehören nach wie vor Flottenbetreiber, Instandhalter, Unternehmen aus der schienengebundenen Güterverkehrslogistik.

Infolge des 2024 vollzogenen Eigentümerwechsels werden keine eigenen IT-Security-Lösungen mehr durch das Unternehmen entwickelt und vertrieben. Infolgedessen gibt es auch keine Business Unit „Systemintegration“ in der ZEDAS GmbH mehr. Die Firma konzentriert ihr Portfolio zukünftig auf Softwarelösungen für die Bahnlogistik und für die Instandhaltung in der Bahn. IT-Sicherheitslösungen gehören nicht zum Kerngeschäft des Unternehmens und werden deshalb nicht mehr aktiv vertrieben.

Des Weiteren ist klar, dass für eine aktive Vermarktung der KI-unterstützten Anomalieerkennung noch beträchtliche Aufwendungen in die

- Weiterentwicklung der KI-Modelle zur Erringung einer größeren Robustheit gegenüber Änderungen in den Prozessdaten sowie
- Softwareentwicklung für eine mögliche Produktreife

getätigt werden müssten. Verschärfend wirken in dieser Situation die am Markt immer schwerer zu bekommenden Softwareentwicklungsressourcen. Das heißt, das vorhandene knappe Personal kann nur für die oben genannten eigenen Kern-Softwareprodukte eingesetzt werden.

Folglich hat sich die Firma entschlossen, trotz des insgesamt erfolgreichen Projektes, die Ergebnisse des Projektes nicht selbst weiterzuentwickeln und zu vermarkten.

2. Vergleich des Vorhabenstands mit der ursprünglichen Planung

In dem Projekt sind folgende Arbeitsschritte des Projektplanes begonnen, bzw. abgeschlossen worden.

Arbeitspaket	Projektschritt	Status
TP 1	Analyse und Konzeption	
AP 1.1	Analyse von Rahmenbedingungen und Spezifikation von Anforderungen	abgeschlossen
AP 1.2	Analyse der Zielsysteme	abgeschlossen
AP 1.3	Grobkonzeption der Anomalieerkennung	abgeschlossen
TP 5	Anforderungen zur Integration in die betriebliche Praxis	
AP 5.1	Datenerhebung und Dokumentation	abgeschlossen
AP 5.2	Anforderungen an Integration und Zertifizierung	abgeschlossen
AP 5.3	Prüfmethoden für Zertifizierung	abgeschlossen
AP 5.4	Planung der Architektur des Demonstrators	abgeschlossen
TP 6	Demonstrator und Evaluation	
AP 6.1	Kombination der Teilmethoden zu einem Demonstrator	abgeschlossen
AP 6.2	Integration in die Betreiberprozesse	abgeschlossen
AP 6.3	Zertifizierungsprüfung der Teilmethoden des Demonstrators	abgeschlossen
AP 6.4	Anwendung, Auswertung und Dokumentation der Ergebnisse	abgeschlossen

Tabelle 1 Bearbeitungsstand der Arbeitspakete

Anhand der Statustabelle ist erkennbar, dass die wesentlichen Arbeitsschritte entsprechend der ursprünglichen Planung abgearbeitet wurden.

3. Die wichtigsten Positionen des zahlenmäßigen Nachweises

Hierzu verweisen wir auf den zahlenmäßigen Verwendungsnachweis.

Bei der Projektdurchführung sind ausschließlich Kosten in Form von Personalkosten (Softwareentwickler, Consultants) entstanden.

4. Die Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Die geleisteten Entwicklungsarbeiten im Projekt waren notwendig und angemessen. Alle wesentlichen, im Arbeitsplan formulierten Aufgaben wurden erfolgreich bearbeitet.

5. Der während der Durchführung des Vorhabens dem ZE bekannt gewordene Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Infolge des Inkrafttretens des novellierten IT- Sicherheitsgesetzes (IT-SiG2.0 vom 18.05.2021) hat die LEAG parallel zu diesem Projekt kommerziell verfügbare Systeme zur Angriffserkennung (SZA) an allen KRITIS- Anlagen der LEAG zum Einsatz gebracht. Laut der Einschätzung der LEAG (Abschlussbericht) hatte WAIKIKI als FuE-Projekt primär die Weiterentwicklung von Wissenschaft und Technik zum Inhalt, während das Einführungsprojekt den allgemein anerkannten Stand der Technik abbildete. In diesem Sinne ergänzten sich beide Vorhaben aus Anwendersicht.

6. Die erfolgten oder geplanten Veröffentlichungen der Ergebnisse

Der entwickelte Demonstrator mit der integrierten KI-gestützten Anomalie-Erkennung wurde auf zwei wichtigen Veranstaltungen vorgestellt, auf der weltgrößten Bahnmesse, der InnoTrans im Jahr 2022 sowie im Jahr 2023, auf dem ZEDAS Summit, an dem fast alle Bestandskunden der ZEDAS-GmbH teilnahmen.

Vorstellung auf Veranstaltungen	Medium
InnoTrans 2022	Workstation
ZEDAS Summit 2023	Workstation

Es gab außerhalb der universitären Veröffentlichungen keine separaten Veröffentlichungen durch die ZEDAS GmbH zu den bisherigen Ergebnissen dieses Projektes.

Darüber hinaus gab es im Rahmen der Projektdurchführung folgende Veröffentlichungen:

1. vgbe KELI 2020 (gemeinsame Veröffentlichung BTU/LEAG) 24./25.11.2020 – Online
2. IMC 2021 - Internet Measurement Conference 02./04.11.2021 – Online (eingereicht)
3. vgbe Fachtagung IT-Sicherheit in Energieanlagen 29.09.2021 – Essen (D)
4. PAM 2022 - Passive and Active Measurement conference 28./29.03.2022 – Online
5. vgbe KELI 2022 (gemeinsame Veröffentlichung BTU/TUC/LEAG) 10./11.05.2022 – Bremen (D)
6. NSS 2023 - International Conference on Network and System Security 14./16.08.2023 – Canterbury (UK)
7. IEEE Access”
Detecting Anomalies in System Logs With a Compact Convolutional Transformer”,
29.09.2023
8. vgbe Fachtagung IT-Sicherheit in Energieanlagen 21.11.2023 – Hamburg (D)

Abbildungsverzeichnis

Abbildung 1 Allgemeines Kommunikationsschema zum Projekt	5
Abbildung 2 Sensor	6
Abbildung 3 Festplatte	6
Abbildung 4 Kommunikationsinfrastruktur der Experimentierplattform	8
Abbildung 5 CPF - Visualisierung Splunk Netzwerkdaten (aggregiert).....	12
Abbildung 6 CPF - Visualisierung Splunk Kontextdaten (aggregiert).....	12
Abbildung 7 CPF - Visualisierung Splunk Anomaliezusammenhang (aggregiert).....	13
Abbildung 8 EXPF – position of the conveyor	13
Abbildung 9 EXPF – light intensity	14
Abbildung 10 EXPF – Kontextdaten Positionierung und Lichtintensität.....	15
Abbildung 11 EXPF – Anomalieerkennung mit Splunk	15

Kurzbericht zum Verwendungsnachweis

Vorhabenbezeichnung: **Verbundprojekt WAIKIKI**

„Wissensbasierte Anomalieerkennung mittels Künstlicher Intelligenz in Kritischen Infrastrukturen“

Teilvorhaben:

Demonstratorentwicklung und Anwendungskordinator für Großanlagen der Energieerzeugung

BMBF-Programm:

IT-Sicherheit - Selbstbestimmt und sicher in der digitalen Welt

Förderkennzeichen: 16KIS1203

Laufzeit des Vorhabens: 01.09.2020 – 31.08.2023

Verlängerung: 01.09.2023 – 31.08.2024

Berichtszeitraum: 01.09.2020– 31.08.2024

Ursprüngliche Aufgabenstellung

Zukunftsfähige Sicherheitslösungen müssen für eine hohe Anzahl von Technologien geeignet sein und die dezentrale Organisation des Energienetzes berücksichtigen. Daher sollen im Vorhaben WAIKIKI Algorithmen des Deep Learning (die vielfältige und komplexe Netzdaten abbilden können) geschickt mit klassischen maschinellen Lernverfahren (die üblicherweise in Lerneffizienz und Analyseperformanz überlegen sind) kombiniert werden, um die Vorteile beider Ansätze optimal auszunutzen. Zudem soll eine Graph-basierte Visualisierung für eine nutzerverständliche Darstellung der trainierten Modelle und Anomalien geschaffen werden und so eine intelligente netzbasierte und nachvollziehbare Anomalieerkennung für Energienetze entstehen.

Ziele sind dabei,

- die Erklärbarkeit der Ergebnisse für die Anwender (Netzbetreiber) herzustellen,
- das effektive Lernen vielfältiger und komplexer Netzkommunikation auf Basis weniger oder unvollständiger Trainingsdaten zu ermöglichen und
- die bisherigen Fehlerraten von selbstlernender Anomalieerkennung auf diesem Gebiet signifikant zu senken.

Die Entwicklung der angestrebten Methoden erfolgt auf Basis realer Daten aus Infrastrukturen von neuer und konventioneller Energieerzeugung sowie höchst modernen Energienetzen (Smart Grids).

Kooperation im Projekt

Mit folgenden wissenschaftlichen Einrichtungen wurde im Rahmen des Projektes kooperiert:

- Brandenburgische Technische Universität Cottbus-Senftenberg (BTU), Lehrstuhl IT-Sicherheit
- Technische Universität Chemnitz, Lehrstuhl Künstliche Intelligenz

Des Weiteren erfolgte die Zusammenarbeit nachfolgend aufgeführten industriellen Partnern:

- ASCORI GmbH, Cottbus
- Migosens GmbH, Mühlheim a. d. R.
- [REDACTED]

Ablauf des Vorhabens

Im Rahmen der Arbeitspakete wurden zunächst die Anforderungen an ein KI-basiertes Anomalie-Erkennungssystem erarbeitet sowie die Nutzerakzeptanzkriterien definiert. Anschließend erfolgte die Planung der zwei benötigten Plattformen, der

- Experimentierplattform,
- Computing Plattform sowie

die Planung der

- Integration der Experimentierplattform bei ASCORI und
- Integration der Computing Plattform [REDACTED] der LEAG.

Nach dem Abschluss der Planungsarbeiten wurden die notwendigen Hardwareteile beschafft, die jeweiligen Plattformen montiert, in ihren geplanten Umgebungen integriert und in Betrieb genommen.

Nachfolgend konnten das Sammeln und Verarbeiten der Sensor- und Kontextdaten sowie das Training der Modelle beginnen.

Die Verarbeitung sowie die Bewertung der Daten starteten nach der Bereitstellung der jeweiligen KI-Modelle durch die BTU-Cottbus-Senftenberg sowie durch die TU-Chemnitz. Parallel begann bereits die Entwicklung des Demonstrators inklusive der notwendigen Auswertungen zur Bewertung der Ergebnisse. Die regelmäßige Evaluation der Ergebnisse aus den KI-Modellen erforderte immer wieder Anpassungsarbeiten am Demonstrator und deren Auswertungen. Diese Arbeiten dauerten bis zum Projektende 08/2024 und auch etwas darüber hinaus an.

Wesentliche Ergebnisse

Die Ergebnisse des Projektes können folgendermaßen zusammengefasst und bewertet werden:

- **Rückwirkungsfreiheit**

- Die Verfahren und Technologien wurden erfolgreich getestet und zeigten laut Aussagen des Praxispartners LEAG keine Rückwirkungen auf die zu überwachenden Leitsysteme.

- **Erkennungsrate und Fehlalarmrate**

- **Erkennungsrate (RPR):** Die Erkennungsgenauigkeit zeigte gute bis sehr gute Ergebnisse, jedoch wurden nur synthetische Angriffsmuster verwendet. Eine weitere Bewertung mit realen Angriffsmustern ist notwendig.
- **Fehlalarmrate (FPR):** Es wurden signifikante Fortschritte erzielt, die Fehlalarmrate konnte deutlich reduziert werden. Dennoch sind weitere Verbesserungen erforderlich und möglich, zum Beispiel durch die weitere Einbeziehung von Kontextinformationen, um letztendlich die Nutzerakzeptanz zu erhöhen.

Genauere Angaben zu Erkennungs- und Fehlalarmraten sind den Berichten und Veröffentlichungen der BTU Cottbus-Senftenberg sowie der TU Chemnitz zu entnehmen.

- **Demonstrator**

- Der Technolgie-demonstrator wird als gelungen und im Rahmen des Projektziels als vollkommen ausreichend bewertet. Natürlich hat der Demonstrator keine Produktreife und ein dauerhafter Einsatz in der Produktion ist in diesem Entwicklungsstand nicht möglich. Das gehörte aber auch nicht zu den Zielen dieses Projektes. In Folgeprojekten müsste entsprechender Aufwand in die Software und das Nutzerinterface gesteckt werden, um das Nutzerinterface einfacher, die Software insgesamt sicherer und die Ergebnisübersichten nachvollziehbarer zu gestalten.

- **Bedienung und Wartung**

- Die Einfachheit in Betrieb und Wartung wurde in dem Projekt nicht ausreichend adressiert und bedarf weiterer Forschung bzw. weiteren Aufwandes. So ist es u.a. wichtig, dass die entwickelten Lösungen mit geplanten Änderungen in den Zielsystemen umgehen können. Eine gute Nutzerakzeptanz erfordert selbstlernende Prozeduren für technische Änderungen. Des Weiteren müssen die verwendeten KI-Methoden sowie die daraus resultierenden Ergebnisse nachvollziehbar und erklärbar sein.

Insgesamt kann man das Projekt als erfolgreich betrachten. Das wird sowohl von der ZEDAS-GmbH als auch von den beteiligten Projektpartnern so eingeschätzt. Die eigentlichen Ziele wurden erreicht. Eine Produkt- und Marktreife zu erzielen, gehörte nicht zu den Projektzielen. Es bedarf erheblicher Aufwendungen in die Entwicklung einer Software, die in robusten Produktionsumgebungen einsetzbar ist.