VDE Studie

Künstliche Intelligenz in der Netzleittechnik

by VDE ETG

VDE

Empfohlene Zitierweise
VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.:
Künstliche Intelligenz in der Netzleittechnik, VDE Studie, Offenbach am Main, Juli 2025

Diese VDE Studie ist das Arbeitsergebnis der VDE ETG Task Force „KI in der Netzleittechnik“.

Autoren:
Jochen Stiasny, TU Delft (Task-Force Leitung)
Markus Mirz, PSI Software SE (Task-Force Leitung)
Mike Vogt, Fraunhofer IEE (Task-Force Leitung)
André Kummerow, Fraunhofer IOSB
Max Dauer, Siemens AG
Janick Meyer, Siemens AG
Heinrich Hoppe-Oehl, Bergische Universität Wuppertal
Michael Igel, Hochschule für Technik und Wirtschaft des Saarlandes
Sarra Bouchkati, IAEW RWTH Aachen
Timon Conrad, Friedrich-Alexander-Universität Erlangen-Nürnberg
Georg Kordowich, Friedrich-Alexander-Universität Erlangen-Nürnberg
Philipp Lutat, IAEW RWTH Aachen
Georgios Mitrentsis, Hitachi Energy
Karsten Viereck, Maschinenfabrik Reinhausen GmbH
Christoph Brosinsky, TEN Thüringer Energienetze GmbH & Co. KG
Klaus Böhme, Siemens AG
Andreas Winter, energis-Netzgesellschaft mbH
Matthias Heinecke, Siemens Energy

Vorbemerkung
VDE Studien geben – entsprechend der Positionierung des VDE als neutraler, technisch-wissenschaftlicher Verband – gemeinsame Erkenntnisse der Mitglieder der Task Force wieder. Die Gemeinschaftsergebnisse werden im konstruktiven Dialog aus häufig unterschiedlichen Positionen erarbeitet. Die Studien spiegeln daher nicht unbedingt die Meinung der durch ihre Mitarbeiterinnen und Mitarbeiter vertretenen Unternehmen und Institutionen wider.

Herausgeber:
VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.
Energietechnische Gesellschaft (ETG)
Merianstraße 28
63069 Offenbach am Main
Tel. +49 69 6308-346
etg@vde.com
www.vde.com/etg

Titelbild: © kras99 - stock.adobe.com

Design: Schaper Kommunikation, Bad Nauheim

Juli 2025

Executive Summary

Die Netzleittechnik steht vor einem Wandel: Künstliche Intelligenz (KI) bietet neue Möglichkeiten zur Optimierung, Effizienzsteigerung und Automatisierung. Doch eine erfolgreiche Einführung erfordert einen strukturierten, ganzheitlichen Ansatz, da viele Akteure und ihre Anforderungen in diesen Prozess einbezogen werden müssen. Dieses Papier bietet eine Orientierung, die drei wesentliche Dimensionen umfasst: technische und regulatorische Rahmenbedingungen, Risiko-Nutzen-Abschätzung und ein vertrauenswürdiger Implementierungsprozess. Da diese drei Aspekte sich gegenseitig beeinflussen und bedingen, müssen sie gemeinsam gedacht werden, um somit KI erfolgreich in der Netzleittechnik einzuführen.

1. **Technische und regulatorische Rahmenbedingungen:** KI bietet vielseitige Anwendungsmöglichkeiten. Der regulatorische Rahmen – insbesondere der EU AI Act – ist jedoch derzeit noch vage. Praxistaugliche Richtlinien müssen noch entwickelt werden, wobei eine enge Zusammenarbeit mit Regulierungsbehörden erforderlich ist. Technisch spielt vor allem die Verfügbarkeit von Daten und deren Qualität eine zentrale Rolle.

2. **Risiko-Nutzen-Abschätzung:** Jeder KI-basierte Lösungsansatz muss sich einer Risiko-Nutzen-Abschätzung stellen, auch im Vergleich mit nicht-KI-basierten Alternativen. Neben potenziellen Vorteilen wie verbessertem Netzbetrieb und Effizienzsteigerung müssen auch operative Risiken und Sicherheitsaspekte berücksichtigt werden. Erfolgreiche Anwendungsfälle zeigen, dass KI signifikanten Mehrwert bieten kann – jedoch nur, wenn Risiken angemessen identifiziert und adressiert werden. Dieses Papier illustriert anhand exemplarischer Anwendungsfälle typische Elemente einer Risiko-Nutzen-Abschätzung beim Einsatz von KI.

3. **Prozessuales Vorgehen für vertrauenswürdige Implementierung:** Die erfolgreiche Anwendung von KI in kritischer Infrastruktur, siehe AI-Act, hängt nicht nur von Technologie und Risiko-Nutzen-Abwägungen ab, sondern es benötigt auch Vertrauen in die neuartigen Methoden. Daher ist eine vertrauenswürdige Integration von KI in die Unternehmensstruktur und Betriebsabläufe entscheidend. Dafür sind klare und überprüfbare Anforderung an KI-Modelle zu formulieren, standardisierte Prozesse zu etablieren und strukturelle Anpassungen vorzunehmen. Die Erfahrungen aus vielen bewährten Prozessen können als Grundlage für KI-spezifische Entwicklungen dienen.

Empfehlungen: Die Einführung von **KI in der Netzleittechnik ist kein Selbstzweck.** Potenziale für viele Anwendungsfälle, sowie bereits in der Praxis eingesetzte Methoden werden in diesem Dokument dargestellt. Jedoch besteht zurzeit das **Risiko einer Überregulierung.** Gleichzeitig ist die Regulierung, speziell der des **EU AI Acts, teils nicht ausreichend konkret,** sodass die Erfüllung der Anforderungen schwer überprüfbar ist. Daher muss in den direkten Austausch mit Regulierungsorganen eingestiegen werden, um auf eine praktisch implementierbare Regulierung hinzuwirken. Ein Kernpunkt dieses Papiers ist unser **Vorschlag wie ein solcher Implementierungsprozess in Anlehnung an etablierte Prozesse aussehen könnte.** Wichtige Voraussetzung für den Einsatz dieses Prozesses ist eine **klare Definition des Anforderungsprofils,** wie in der Sektion „Vertrauen schaffen durch einen Implementierungsprozess" beschrieben.

Für Netzbetreiber und andere Akteure empfehlen wir einen schrittweisen Einstieg, beginnend mit **Anwendungsfällen geringeren Risikos oder gut überprüfbaren KI-Methoden.** Bei der Auswahl derartiger Anwendungsfälle unterstützt unsere Darstellung. **Qualifiziertes Personal sollte auch bei zunehmendem KI-Einsatz die letzte Entscheidungsinstanz** bleiben und durch gezielte Schulungen befähigt werden, KI-Empfehlungen kompetent zu bewerten.

Inhaltsverzeichnis

1 Einleitung

Die Transformation des Stromnetzes im Zuge der Dekarbonisierung erfordert eine moderne und leistungsfähige Netzleittechnik. Sie spielt eine zentrale Rolle bei der **Bewältigung zunehmender Komplexität der Stromnetze**, der effizienteren Nutzung bestehender Infrastrukturen, sowie der Erfüllung regulatorischer Vorgaben. Ein wichtiger Schritt auf diesem Weg ist die **verstärkte Automatisierung**, wie sie im Impulspapier [1] anhand verschiedener Anwendungen aufgezeigt ist. Ergänzend zu diesen Vorschlägen wird die Nutzung von KI als funktionale Erweiterung im Rahmen dieses Papiers betrachtet.

Das **Potential KI-basierter Methoden** entstammt der Möglichkeit, **große Datenmengen** effizient zu verarbeiten, Zusammenhänge aufzudecken und hochkomplexe Zusammenhänge kompakt abzubilden. Zudem können im Trainingsprozess zusätzliche Informationen integriert werden, sodass auch unvollständige Daten sinnvoll genutzt werden können. Diese technischen Potenziale lassen sich in der Netzleittechnik sowohl zur Optimierung bestehender Funktionen als auch zur Erschließung neuer Anwendungsfelder einsetzen.

Die praktische Einführung von KI im Bereich der **Kritischen Infrastrukturen (KRITIS)** insbesondere im Anwendungsfeld der Netzleittechnik gestaltet sich als herausfordernd. Erfahrungswerte im Umgang mit KI fehlen in vielen KRITIS Unternehmen, unter anderem weil hier **strenge Anforderungen** zur Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen gelten. Weitere Hürden zur Einführung von KI-Anwendungen sind unter anderem eine begrenzte **Verfügbarkeit und Qualität von Daten**, Schwierigkeiten bei der organisatorischen Integration, fehlendes Know-how sowie mangelndes Vertrauen in die durch KI-Anwendungen erzeugten Entscheidungsvorlagen.

Für die vollständige Entfaltung der Potenziale von Künstlicher Intelligenz ist es notwendig **unterschiedlichste Experten** (Daten-Analysten, Software-Entwickler, Domänen-Experten) und Abteilungen (Asset, System, Finanz, IT) in die Projekte zu integrieren. Aus diesem Grund sind KI-Projekte oftmals auch **Organisationsentwicklungsprojekte** welche einen starken Fokus auf interne Prozesse, Verantwortlichkeiten und insbesondere Change-Management legen sollten.

Eine umfassende Behandlung all dieser Aspekte würde den Rahmen dieses Dokuments sprengen; daher wird an dieser Stelle auf die Arbeit weiterer Arbeitsgruppen und deren Veröffentlichungen, soweit bereits vorhanden, verwiesen – siehe DKE/AK 901.0.42 KI in der Energietechnik, CIGRE Working Group C2.42 [2], VDE ETG Arbeitsgruppe zu Digitalen Zwillingen [3] bezüglich organisatorischer Aspekte.

Dieses Dokument verfolgt das Ziel, einen strukturierten Rahmen für die Entwicklung, Bewertung und Implementierung KI-gestützter Ansätze in der Netzleittechnik abzubilden. Es richtet sich insbesondere an Netzbetreiber, Hersteller und Forschende, die sich strategisch mit dem Einsatz von KI auseinandersetzen. Dabei werden drei zentrale Dimensionen betrachtet:

- **Technische und regulatorische Rahmenbedingungen:** Welche Herausforderungen sind bei der Einführung von KI-Methoden zu berücksichtigen?
- **Risiko-Nutzen-Abschätzung**: Welche Risiken und Potenziale lassen sich aus konkreten Anwendungsfällen ableiten?
- **Prozessuales Vorgehen für vertrauenswürdige Implementierung:** Wie kann die Einführung neuer KI-basierter Methoden in die Netzleittechnik nachhaltig und vertrauenswürdig gestaltet werden?

2 Stand heute – Regulatorik und technische Randbedingungen

Regulatorik

Aufgrund der ungenauen Definition und der breiten Verwendung des Begriffs „künstliche Intelligenz“ variieren die Interpretationen und Identifizierungen von Technologien als KI-Technologien zwischen verschiedenen Forschungsdisziplinen. Es ist daher nicht verwunderlich, dass Gesetzgeber, Wissenschaftler, Industrieverbände, Gremien, Ausschüsse und Medien noch keine eindeutige gemeinsame Kategorisierung gefunden haben und dass unter KI das verstanden wird, was der allgemeine und der mediale Sprachgebrauch vorgibt. Eine aktuelle Darstellung von Einsatzmöglichkeiten von KI im sogenannten „Smart Grid” ist in [4] zusammenfassend beschrieben. Ein ausführliches Glossar zu Begrifflichkeiten im Kontext von KI ist hierin ebenfalls zu finden, um deren Bedeutung zu erläutern.

In der Wissenschaft und Normung wird der Begriff KI näher betrachtet, indem Unterklassen und Technologiegruppen definiert werden, wohingegen in den Medien teilweise nur die General Purpose Artificial Intelligence wie bspw. ChatGPT als KI bezeichnet wird. Für Mathematiker indes zählen auch bereits lange etablierte Methoden, wie Regressionsverfahren in den Bereich der KI-Methoden.

Dieser Konflikt spiegelt sich zusätzlich in der Diskussion um Regulatorik und Gesetzgebung wider: Die aktuelle Definition im EU AI Act („KI-System”) ist schwach und ohne echte Eingrenzung formuliert, um eine Festlegung auf sprachlich umrissene Einzel-Technologien zu vermeiden. Die Definition folgt einer von der OECD festgelegten Sprachverwendung. Diese Festlegung führt zu dem Ergebnis, dass ein großer Teil europäischer Software-Produkte adressiert wird, ohne dass in ihnen neuartige KI-Methoden Verwendung finden. Das Risiko einer Überregulierung existiert und eine entsprechende Kritik findet sich in verschiedenen technisch-juristischen Veröffentlichungen [5]. Eine resultierende Herausforderung für Unternehmen liegt darin, das Compliance Management auf eine Vielzahl von Softwareprodukten ausdehnen zu müssen. Eine technische Definition des KI-Begriffs wäre daher wünschenswert, um diese Auswirkungen in der Unternehmenspraxis zu vermeiden. Eine Orientierung bietet diesbezüglich die Normungs-Roadmap zu KI für die deutsche Industrie [6] und die dena-Analyse zum Einsatz von KI in der Energiewirtschaft [7].

Neben der Eingrenzung des KI-Begriffs besteht eine weitere Herausforderung darin, dass die Anforderungen für die Einführung von KI-Methoden in der Regulatorik Interpretationsspielraum zulassen. Beispielsweise hängen diese Anforderungen davon ab, ob es sich um einen Hochrisiko-Anwendungsfall handelt, wobei unklar ist ob tatsächlich jeder Einsatz von KI in einer kritischen Infrastruktur ein hohes Risiko darstellt. Zudem erschweren die Spielräume in der Definition der technischen Dokumentation es, der Dokumentationspflicht nachzukommen. Tabelle 1 bietet eine Übersicht zur risikobasierten Kategorisierung.

Risiko	Regulierungsanforderung	Verhaltensempfehlung / Verpflichtung	Anwendungsbeispiel
Minimalrisiko	Unreguliert	Ein Verhaltenskodex wird empfohlen	Videospiele, Spam Filter
Begrenztes Risiko	geringe Transparenzverpflichtungen	Entwickler und Betreiber müssen sicherstellen, dass die Endnutzer wissen, dass sie mit KI interagieren	Chat Bots, Deep Fakes, Interne Modelle
Hoch-Risiko	Systeme mit hohem Risiko sind zulässig, müssen aber umfassenden Anforderungen genügen	Dokumentationspflichten und Transparenzanforderungen müssen von den Anbietern/Betreibern von KI-Systemen mit Einsatzbereichen, die in den Hoch-Risiko Bereich fallen erfüllt werden	KI-Systeme, die als Sicherheitskomponenten für die Verwaltung und den Betrieb kritischer digitaler Infrastrukturen, für den Straßenverkehr oder für die Wasser-, Gas-, Wärme- oder Stromversorgung eingesetzt werden sollen
Unannehmbar/ Inakzeptabel	Einsatz nicht erlaubt	Der Einsatz von KI-Systemen, welche ein inakzeptables Risiko darstellen ist nicht gestattet	soziale Bewertungssysteme, manipulative KI, Biometrische Identifizierung in Echtzeit, Emotionserkennung am Arbeitsplatz

Tabelle 1: Risikobasierte Kategorisierung von KI-Systemen nach EU AI Act [8]

Technische Randbedingungen

Aus Perspektive der technischen Realisierbarkeit gibt es bereits einige Beispiele für verfügbare KI-Anwendungen in der Energiewirtschaft:

- Angriffserkennung, Zeitreihenanalyse und Prognose [9], [10],
- Vorausschauende Instandhaltung (Predictive Maintenance) [11],
- Bilderkennung z.B. zur Einmessung von Hausanschlüssen,
- Drohnenflüge zur Erfassung des Zustands von Freileitungen und zur Bewuchserkennung [12], [13],
- Anomalieerkennung [14], z.B. im Bereich Abrechnungen wegen eines stark veränderten Kundenverhaltens im Kontext der Gas-Krise [9] oder Prozessanomalien [15].

Daran lässt sich auch erkennen, dass KI-Methoden auf eine immer größer werdende Vielfalt von Daten angewendet werden können und zunehmend Einzug in die Energiewirtschaft halten.

Festzuhalten ist, dass ein zentraler Faktor für den erfolgreichen Einsatz von KI-Methoden und Machine Learning Methoden im speziellen, die Verfügbarkeit entsprechender Trainingsdaten ist. Insbesondere bei der Netzleittechnik muss frühzeitig bedacht werden, dass die Kommunikationstechnik zwischen Geräten in der Prozessebene und dem verarbeitenden, eventuell zentralen, System bei bestimmten Anwendungsfällen eine Herausforderung darstellt.

Die zentralen Komponenten der Netzleittechnik umfassen das Leitsystem mit SCADA Anwendungen, die Stationsautomatisierung bis hin zur Feldleitebene und die dazwischen liegende Fernwirktechnik, wie in Abbildung 1 dargestellt. Die wesentlichen Aufgaben des Leitsystems bzw. der Leitstelle und deren derzeitiger Automatisierungsgrad, sowie die Ziele weitergehender Automatisierung werden in [1] dargestellt. Diese Ziele umfassen beispielsweise die Beherrschung der zunehmenden Komplexität, die effiziente der Ausnutzung der Infrastruktur und die Unterstützung bei regulatorischen Anforderungen.

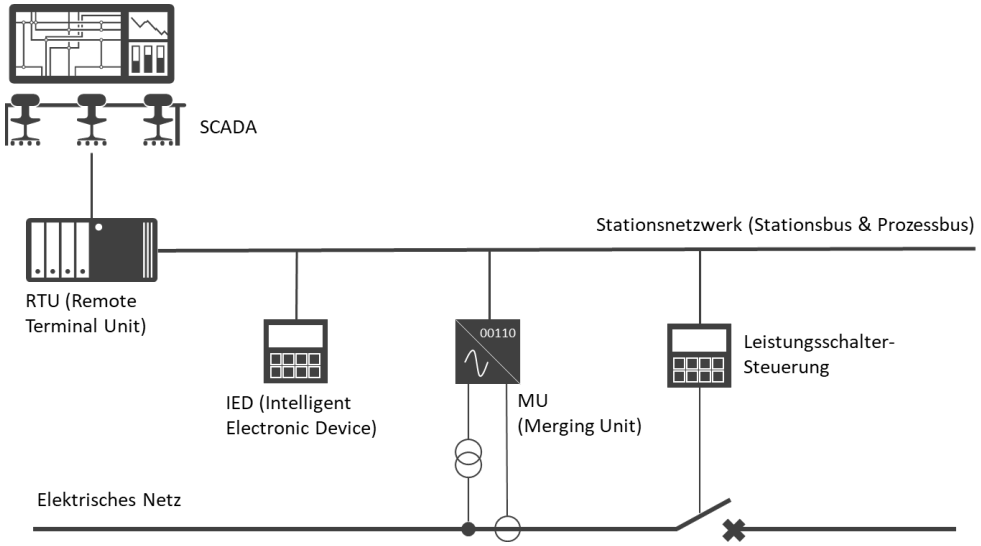

Abbildung 1: Leitsystem mit SCADA Anwendungen, Prozessankopplung und Stationsautomatisierung

Um unnötige Datenübertragung zu minimieren, gilt es, Informationen so weit wie möglich in der Feldleitebene oder Stationsleitebene zu verarbeiten, oder die Fernwirktechnik den neuen Anforderungen entsprechend auszulegen. Dies muss sowohl für das Sammeln von Trainingsdaten wie auch für die letztliche Anwendung der KI-Methode bedacht werden. Beispiele für datenintensive Anwendungen in Stationen, anhand derer man diese Schwierigkeiten erkennen kann, sind Asset-Performance Management Systeme, z.B. für die Zustandsanalyse von Komponenten mit Hilfe von Vibro-Akustik [16]. Weitere Anwendungsfälle mit ihren Stärken und Herausforderungen werden im Folgenden dargestellt.

3 Potenziale von KI in der Netzleittechnik anhand einiger Anwendungsfälle

Um zu illustrieren, wie KI-Methoden in der Leittechnik gewinnbringend eingesetzt werden können, werden im folgenden Abschnitt verschiedene Anwendungsfälle vorgestellt. Hierbei wird der Fokus auf den Mehrwert von KI-Systemen innerhalb dieser Anwendungsfälle und auf die Darstellung von etwaigen Risiken gelegt. Die ausgewählten, in Tabelle 2 aufgeführten Beispiele dienen der Illustration, ohne einen Anspruch auf Vollständigkeit zu erheben.

Anwendung	Zweck der Anwendung	Bereitstellung	Art des Mehrwerts
Prognose Last und Erzeugung	Vorhersage der Solar- und Windeinspeisung sowie von Lasten mithilfe von Wetterprognosen und -kameras	Zentral	Verbesserung von (regionalen) Vorhersagen
Anomaliedetektion	Analyse von Messdaten für die Früherkennung von Fehlern	Edge	Erhöhung der Resilienz des Energiesystems und der Betriebssicherheit
Angriffserkennung	Erkennung von Manipulationen in Messwerten oder in der Kommunikation zwischen Leit- und Feldebene	Zentral	Erhöhung der Resilienz des Energiesystems und der Betriebssicherheit
Assistentensystem in der Systemführung	Chat-basierte Unterstützung des Systemführers zur Entscheidungsfindung durch schnelle Bereitstellung benötigter Informationen aus internen Unternehmensdaten oder externen Quellen oder Aufmerksamkeitslenkung durch hervorheben von Informationen	Zentral	Entlastung des Personals und schnellere Einarbeitungszeiten in komplexe Systemführungsaufgaben
Zustandsschätzung in der Niederspannung	Vermeidung von Engpässen und normativ unzulässigen Netzzuständen durch einen kostenminimierten Einsatz von flexiblen Lasten und Einspeisern	Zentral	Überwachung und Optimierung des Netzzustandes bei minimaler Ausrüstung mit Messsystemen
Schutzparameteroptimierung	Automatisierte Parametrierung, Bewertung und Optimierung von Schutzkonzepten basierend auf Meta-Heuristiken	Zentral oder Edge	Reduktion Personalaufwand, höhere Netzsicherheit, bessere Netzauslastung
Zentrale Kurzschlussortung (post mortem)	Identifikation von betroffener Leitung und Lokalisation Kurzschlussort	Zentral oder Edge	Minimale Ausstattung mit Messystemen, schnellere Fehlerklärung

Edge: Verarbeitung nah an Feldgeräten, beispielsweise in der Stationsleittechnik
Zentral: Verarbeitung in einer zentralen Leitstelle on-premise oder in einer public Cloud

Tabelle 2: Anwendungsgebiete für KI in der Netzleittechnik

In Abbildung 2 ist der Zeithorizont dargestellt, in dem sich die jeweiligen Anwendungsfälle implementieren lassen. „Kurzfristig“ bezeichnet hierbei Anwendungsfälle, die bereits im Einsatz sind oder kurz vor der Implementierung stehen (Zeithorizont 1 Jahr), während „Mittelfristig“ in naher Zukunft (Zeithorizont 3...5 Jahre) implementiert wird und „Langfristig“ Anwendungsfälle, die zwar ein hohes Potenzial bieten, aber noch erhebliche Weiterentwicklungen und ggfs. Forschung erfordern, bevor sie eingesetzt werden können (Zeithorizont 10 Jahre).

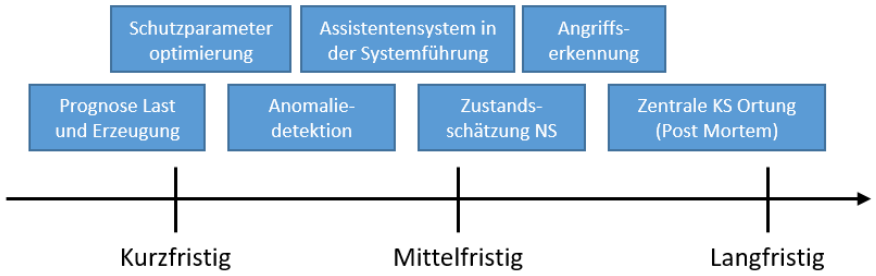

Abbildung 2: Zeithorizont für den Einsatz von KI-Methoden für die beschrieben Anwendungsfälle

Der Mehrwert der vorgestellten KI-Anwendungen kann vorrangig in zwei Kategorien unterteilt werden. Einerseits kann der Einsatz von KI bereits **bestehende Funktionen verbessern.** Die Verbesserung kann sich hierbei entweder auf die Qualität oder auf die benötigte Zeit einer Funktionsausführung beziehen. Die qualitative Verbesserung einer bestehenden Funktion wird durch den Anwendungsfall „Lastvorhersage" veranschaulicht, während die Beschleunigung einer bereits bestehenden Funktion durch den Anwendungsfall „Schutzparameteroptimierung" repräsentiert ist. Andererseits können KI-Methoden auch **grundsätzlich neue Funktionen** ermöglichen, die zuvor mit klassischen Methoden schlicht nicht umsetzbar waren. Beispiele hierfür sind die Detektion von Anomalien in Messdaten, die zuvor nicht durch klassische Verfahren der Schutztechnik erkannt wurden oder ein Beratungsassistent für die Systemführung, der erst durch das Aufkommen von Large Language Models (LLMs) ermöglicht wird.

Nicht nur Vertrauenswürdigkeit, sondern auch das Thema Transparenz spielt bei der Bewertung von KI-Anwendungen eine große Rolle. Dies betrifft insbesondere für den Betrieb relevante Aspekte wie die schnelle und intuitive Nachvollziehbarkeit von KI-Entscheidungen, die Einführung von Kontrollparametern oder der effiziente Umgang mit fehlerhaften KI-Ergebnissen und Möglichkeiten zur Ursachenbehebung. Abbildung 3 stellt das Risiko eines Einsatzes von KI-Anwendungen dar. Als besonders geeignet stechen KI-Systeme hervor, bei denen entweder die Qualität der Funktion gut überprüft werden kann, oder bei denen die Folgen eines Fehlers als eher gering eingeschätzt werden können. Ein genereller Überblick zu Risiken, die beim Einsatz von KI-Methoden bestehen, wird in [17] gegeben.

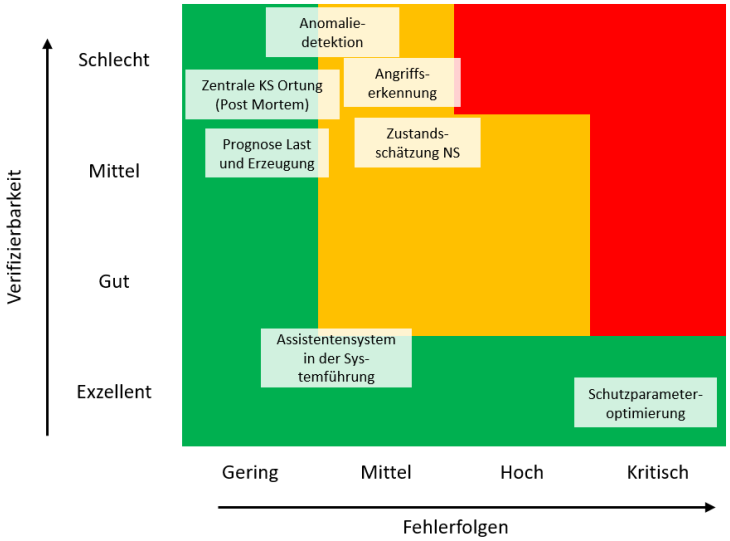

Abbildung 3: Einordnung der beschriebenen Anwendungsfälle in einer Risiko -Matrix entlang der Folgen, die eine falsche oder ungenaue Modellausgabe hat, und der Möglichkeit die Modellausgabe auf die Genauigkeit der Funktion zu überprüfen.

Vorstellung der exemplarischen Anwendungsfälle

Prognose Last und Erzeugung

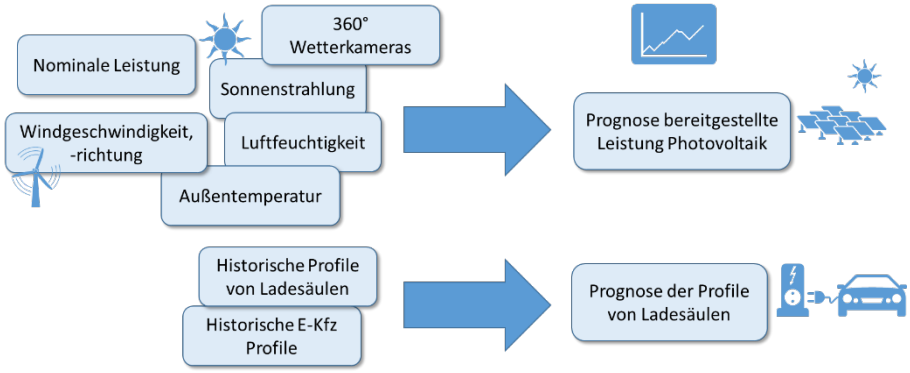

Abbildung 4: Prognose Last und Erzeugung

Beschreibung & Mehrwert: Die Vorhersage bzw. Prognose von Last und Erzeugung hilft dabei einen sicheren Betrieb des elektrischen Energieversorgungsnetzes zu gewährleisten. KI-Modelle können schneller Prognosen erstellen als physikalische Modelle, sind aber auch durch die Güte von Wetterprognosen limitiert. Zur Prognose der bereitgestellten Leistung einer Photovoltaikanlage (PVA) werden dabei Daten zu Außentemperatur, globale Sonnenstrahlung, Windgeschwindigkeit, Windrichtung und Luftfeuchtigkeit sowie der nominalen Leistung verwendet. Wird die PVA mit 360° Wetterkameras ausgestattet, können sehr kurzfristige Prognosen zur bereitgestellten Leistung der Photovoltaikanlage erstellt werden.

Mithilfe von historischen Daten zum Energiebezug von Ladesäulen und E-Kfz können entsprechende Profile erstellt werden. Versuche erzielten bei der Prognose des Energiebedarfs für einen Tag an einer Ladesäule gute Genauigkeiten.

Umgang mit Risiko: Ungenaue Prognosen zu Last und Erzeugung können zu Problemen bei der Prognose des Netzzustandes führen, wodurch weitere Kosten entstehen, denn diese Differenzen müssen an kurzfristigen Energiemärkten ausgeglichen werden. Der Umgang mit Risiken ist ähnlich zu klassischen Prognosealgorithmen, denn klassische physikalische Modelle weisen ebenfalls Prognoseunsicherheiten auf.

Integration in Infrastruktur: Daten zur nominalen Leistung von PVA und dem Energiebezug von E-Kfz an Ladesäulen stehen bei den jeweiligen Betreibern zur Verfügung. Wetterdaten können von (lokalen) Wetterdienstleistern bezogen werden. Nach Aufbereitung der Daten können mit diesen direkt KI-Modelle trainiert werden.

Fazit: KI-Modelle zur Prognose von Zeitreihen, z.B. der bereitgestellten Leistung einer PVA, bieten eine teilweise höhere Genauigkeit als physikalische Modelle (siehe dazu [18]). Wie in Abbildung 2 dargestellt, befinden sich solche Systeme bereits im Einsatz und werden kontinuierlich verbessert.

Anomaliedetektion

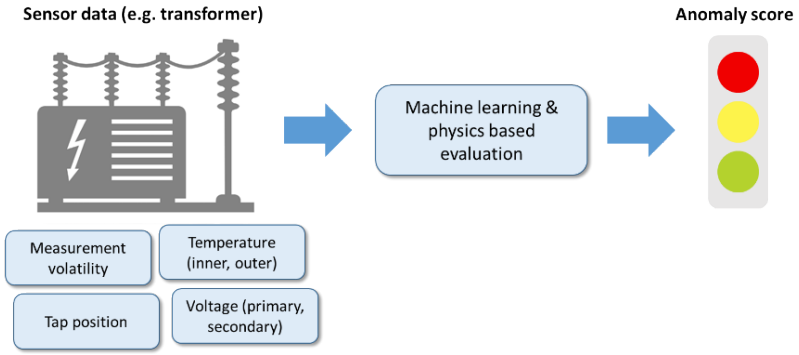

Abbildung 5: Anomaliedetektion

Beschreibung & Mehrwert: Die Detektion von Anomalien erlaubt eine erweiterte Analyse von Messdaten, die über die traditionelle Schutztechnik hinaus auch weniger schwerwiegende Ereignisse detektieren kann. Auch wenn der direkte Einfluss solcher Anomalien als eher gering einzuschätzen ist, kann die Identifikation dieser einen hohen Mehrwert bieten. Als Beispiel ist hierbei die Erkennung von sehr hochohmigen Erdfehlern anzuführen, die jedoch trotz der geringen Ströme langfristig Brände auslösen können oder zu Verschmutzung bzw. Schwächung von Isolation und nachfolgend zu einem Überschlag führen kann [19]. Eine frühzeitige Detektion ermöglicht das Einleiten von Gegenmaßnahmen. Auch zur Detektion von Anomalien in Transformatormessdaten wurden KI-Systeme bereits eingesetzt [20].

Umgang mit Risiko: Die Rolle dieser erweiterten Systeme ist klar abgegrenzt. Sie dienen nicht der sofortigen Abschaltung bei einem Fehler, sondern liefern ergänzende Informationen an menschliche Betriebsführer. Die zusätzlichen Informationen können als Ergänzung zur bestehenden Schutztechnik betrachtet werden, ohne dass der Einsatz von KI hierbei ein Risiko für den sicheren Betrieb der kritischen Infrastruktur darstellt. Aus diesem Grund ist das Risiko des Anwendungsfall in Abbildung 3 als gering eingestuft.

Integration in Infrastruktur: Insbesondere die Nutzung des IEC 61850 Standards sowie sogenannte „centralized protection and control“ (CPC)-Hardware ermöglichen die Erfassung der Daten vom Stationsbus und die Auswertung mit KI-Algorithmen. Entscheidend ist hierbei, dass der Einsatz der KI auf einem Edge-Device erfolgt, ohne die Notwendigkeit hochaufgelöste Datenströme in die Leitwarte zu übertragen. Die Patch- und Updatestrategie kann für solche Systeme analog zur klassischen Schutztechnik umgesetzt werden.

Fazit: Um ein solches System sinnvoll einsetzen zu können ist die Generalisierungsfähigkeit der KI-Algorithmen essenziell. Hierfür ist ein möglichst diverser Trainingsdatensatz erforderlich. Ebenso wichtig ist ein Benchmark Datensatz wie beispielsweise in [21], der die Realität möglichst akkurat repräsentiert, um die KI-Algorithmen gut evaluieren zu können.

Angriffserkennung

Beschreibung & Mehrwert: Der Einsatz von KI-Methoden zur Angriffserkennung im Leitsystemumfeld bietet großes Potenzial, um den Betrieb kritischer Infrastrukturen sicherer und widerstandsfähiger gegenüber Cyberbedrohungen und technischen Fehlern zu gestalten. Besonders dort wo automatisierte Steuerungssysteme eingesetzt werden, ist der Schutz vor Angriffen essenziell.

Ähnlich zur Anomalieerkennung ermöglichen moderne KI-Verfahren die frühzeitige Erkennung von Manipulationen in Messwerten sowie bei deren Übertragung von der Feld- in die Leitebene. Durch den gezielten Einsatz von maschinellem Lernen oder Deep Learning lassen sich verdächtige Muster identifizieren, die auf fehlerhafte Sensorik oder gezielte IT-Angriffe hindeuten. Dies bietet eine zusätzliche Sicherheitsebene über klassische Ansätze hinaus.

Ein besonders vielversprechender Ansatz ist die kombinierte Auswertung von Prozess- und Kommunikationsdaten. Im Gegensatz zur herkömmlichen Grenzwertprüfung oder Bad-Data-Detection kann durch KI-gestützte Verfahren besser zwischen technischen Störungen und IT-basierten Angriffen un-

terschieden werden. So wird die Reaktionsfähigkeit auf Vorfälle verbessert und der Netzbetrieb kann robuster abgesichert werden.

Umgang mit Risiko: Eine Herausforderung ist die Minimierung von fälschlicherweise erkannten Anomalien. Dies ist insbesondere bei auftretenden Prozess- oder Konfigurationsänderungen kritisch und muss für Trainings- sowie Betriebsprozess bedacht werden. Es ist neben der Meldung erkannter Anomalien auch die zusätzliche Angabe von Anomalie- oder Angriffsursachen notwendig, um passende Gegenmaßnahmen im Leitsystem oder Security Operations Center (SOC) abzuleiten und fehlerhafte Reaktionen zu vermeiden.

Integration in Infrastruktur: Für die zusätzliche Erfassung von Kommunikationsdaten kann auf bestehende (dezentrale) Security Information and Event Management (SIEM)-Sensoren in der Prozess-IT zurückgegriffen werden. Die Verschneidung und Auswertung der Prozess- und Kommunikationsdaten erfordern die Umsetzung eines gesonderten Datenaustauschs mit entsprechenden Zugriffen für Betriebs- und IT-Verantwortliche.

Fazit: Wie auch im Fall der Anomalieerkennung ist eine umfassende und repräsentative Datenbasis essenziell zur Erreichung einer ausreichend hohen Detektionsqualität der Angriffserkennung. Ohne Einsatz von KI ist eine kombinierte Auswertung von Prozess- und Kommunikationsdaten nicht sinnvoll möglich. Die zunehmende Anzahl an Angriffen auf kritische Infrastrukturen sowie die zunehmende Integration von IoT-Technologien erhöht die Notwendigkeit Kommunikationsdaten explizit in die Netzbetriebsüberwachung zu integrieren. Erste KI-basierte Industrielösungen werden bereits zur Überwachung von SCADA-Daten [22] oder zur Angriffserkennung durch OT-nahe SIEM-Systeme [23] angeboten.

Assistentensystem in der Systemführung

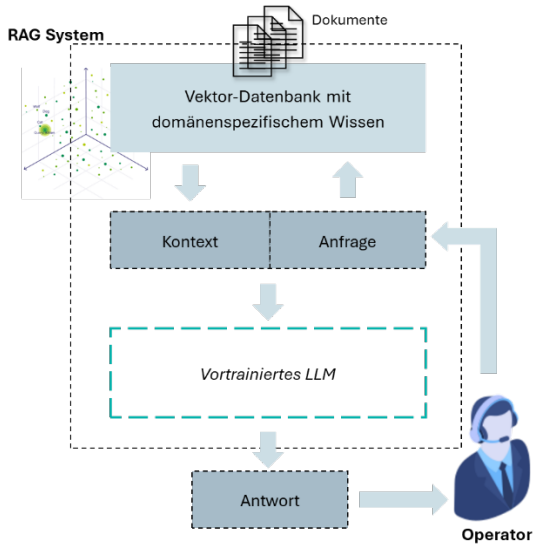

Abbildung 6: Assistentensystem in der Systemführung

Beschreibung & Mehrwert: Sprachmodelle wie ChatGPT haben einen weiten Einzug in Unternehmen erhalten und können auch in der Systemführung einen deutlichen Mehrwert in Form einer Chat-basierten Assistenz für das Personal darstellen. Über sogenannte Retrieval Augmented Generation (RAG)-Systeme können auf Benutzeranfrage relevante Informationen aus verschiedenen Dokumenten, z.B. interne Vorschriften, technische Dokumentationen oder Standards, miteinander verknüpft und zur Verfügung gestellt werden. Somit können Systemführer Unterstützung erhalten beim Umgang mit kritischen oder komplexen Betriebssituationen, bei der Einarbeitung in neue Betriebsanforderungen oder bei der effizienten Aufbereitung und Vermittlung von Erfahrungswissen. Generative KI wird zunehmend in autonome Agentensysteme eingebettet, die in der Lage sind, bei komplexen Aufgaben als Berater, Analysten oder Entscheidungshilfen zu agieren. Diese Agentenrolle kann grundsätzlich auch im Leitsystemumfeld eingebettet werden, sofern die entsprechenden Voraussetzungen erfüllt sind und das Vertrauen in die Technologie vorhanden ist. Somit könnten autonome KI-Agenten zukünftig im Zusammenspiel mit menschlichen Operatoren Netzsituationen analysieren, Handlungsempfehlungen geben und Teilentscheidungen autonom treffen. Letztlich wird jedoch der Mensch in seiner Rolle als

Systemführer die implementierten Entscheidungen verantworten müssen und somit Teil dieser Aufgabe bleiben [24].

Umgang mit Risiko: Sprachmodelle tendieren zu allgemeinen Aussagen und können bei fehlendem Wissen halluzinieren. Das heißt sie generieren fehlerhafte oder ungenaue Ausgaben. Dies kann durch eine genaue Kalibrierung des RAG-Systems inkl. einer korrekten Extraktion der Dokumente minimiert werden. Dennoch sollte das entsprechende Personal im Umgang mit Sprachmodellen geschult werden.

Integration in Infrastruktur: Insbesondere beim Einspielen unternehmensinterner Dokumente sowie beim Informationsaustausch zwischen RAG-System und Sprachmodell sollten datenschutzrechtliche Anforderungen und klare Rollenzuweisungen beachtet werden. Darüber hinaus werden umfangreiche Tests unter Verwendung ausgewählter Anwendungsbeispiele benötigt, um die Ausgaben des LLM/RAG-Systems entsprechend den eigenen Bedürfnissen zu optimieren. Dies setzt auch eine umfassende Pflege und Aufbereitung insbesondere unternehmensinterner Dokumente oder Wissensdatenbanken voraus.

Fazit: Sprachmodelle in Verbindung mit RAG-Systemen können bisher ungenutzte Datenpotenziale für die Betriebsführung nutzbar machen und stellen eine gute Ergänzung dar zu sensorgetriebenen Anwendungen, wie z.B. Prognosen. Bei korrekter Nutzung und Kalibrierung solcher Systeme sind auch langfristige positive Effekte auf die Arbeitsweise und Aufgaben von Betriebsführern zu erwarten. Der Einsatz von generativer KI und LLMs bietet hohes Potenzial für die Netzleittechnik – sowohl operativ als auch strategisch. Sie könnte die Netzführung präziser, resilienter und effizienter machen – vorausgesetzt, Herausforderungen wie Halluzinationen und Validität der Ergebnisse werden zuverlässig adressiert. Über eine Vielzahl an Software-Frameworks, z.B. Langchain [25], oder Service-Anbietern können RAG-Systeme verhältnismäßig einfach unter Einbeziehung von Open-Source-Sprachmodellen, z.B. das europäische Sprachmodell Teuken-7B [26], aufgesetzt werden.

Zustandsschätzung in der Niederspannung

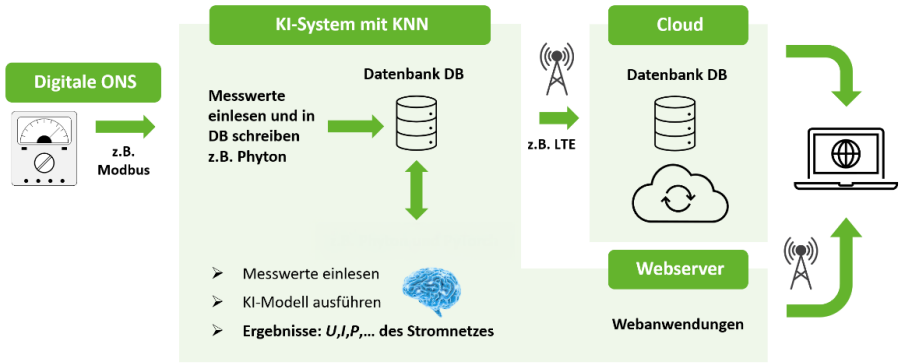

Abbildung 7: Zustandsschätzung in der Niederspannung

Beschreibung & Mehrwert: Für die Gewährleistung einer stabilen und sicheren Stromversorgung ist die kontinuierliche Kenntnis des aktuellen Zustands der Stromverteilnetze von essenzieller Bedeutung. Insbesondere die hohe Anzahl sowie die weitreichende geografische Ausdehnung der Verteilnetze – vor allem im Bereich der Niederspannung – erfordern die Entwicklung kosteneffizienter und skalierbarer Monitoring Lösungen. Die Beobachtbarkeit der Niederspannungsnetze ist bislang aufgrund fehlender Messsysteme nur in begrenztem Maße gegeben. In diesem Kontext bieten KI-basierte Systeme zur Zustandsidentifikation und Betriebsüberwachung ein hohes Potenzial. Ein wesentlicher Vorteil dieser Systeme liegt in den geringen Anforderungen an Rechenleistung und Speicherressourcen, wodurch eine Implementierung auf kostengünstiger, dezentral platzierter Hardware außerhalb zentraler Leitwarten ermöglicht wird.

Umgang mit Risiko: Der Einsatz KI-basierter Zustandsschätzungen ist derzeit mit geringem Risiko verbunden, da solche Verfahren in der Niederspannung bislang kaum Anwendung finden und daher keine etablierten Prozesse beeinträchtigt werden können.

Integration in Infrastruktur: KI-basierte Systeme bieten die Möglichkeit, sowohl dezentrale Lösungen mit kostengünstiger Hardware direkt in Ortsnetzstationen als auch zentrale Anwendungen in Leitstellen

umzusetzen. Für das Training solcher Systeme ist eine vollständige netzphysikalische Beschreibung erforderlich. Das bedeutet, dass sämtliche relevanten Parameter des Stromnetzes bekannt und korrekt erfasst sein müssen, um eine zuverlässige Modellbildung zu gewährleisten. Dabei ist insbesondere auf die Qualität, Aktualität und Zuverlässigkeit der verwendeten Datenquellen zu achten. Unabhängig vom konkreten Einsatzzweck stellen unvollständige oder inkonsistente Daten – insbesondere im Bereich der Niederspannungsnetze – eine zentrale Herausforderung dar, die die Leistungsfähigkeit datenbasierter Systeme beeinflussen kann.

Fazit: Erste Feldversuche im Rahmen des BMWK-Verbundvorhabens GridAnalysis [27] in einem Niederspannungsnetz haben bestätigt, dass eine KI-basierte Zustandsschätzung von Stromverteilnetzen im optimalen Fall nur die Verarbeitung der in den Ortnetzstationen gemessenen Spannungen und Leistungen benötigt und keine weiteren Messdaten aus dem übrigen Stromverteilnetz erforderlich sind. Die dabei erzielten Schätzgenauigkeiten liegen im Bereich der Messgenauigkeit handelsüblicher Messtechnik und belegen somit das Potenzial dieser Methode für eine praxistaugliche Anwendung.

Schutzparameteroptimierung

Beschreibung & Mehrwert: Nie zuvor haben sich Energienetzte so stark verändert wie aktuell. Dabei mangelt es an Schutzingenieuren, die Veränderungen überprüfen und notwendige Anpassungen an Schutzeinstellungen vornehmen. Es bedarf daher eines Systems, welches Schutzkonzepte voll automatisiert bewertet und abhängig der Ergebnisse optimiert. Hierbei kommt ein Particle Swarm Optimization (PSO) Algorithmus zum Einsatz, der sowohl in den Bereich der Metaheuristik als auch der KI fällt. Der Algorithmus erlaubt die koordinierte Einstellung verschiedener Schutzfunktionen auf verschiedenen Schutzgeräten eines systemweiten Netzes durch Anpassung von Parametern wie Reaktanzen, Stromschwellen oder Auslösezeiten. Ziel ist es, die klassischen Schutzkriterien Selektivität, Zuverlässigkeit und Sicherheit zu verbessern, aber auch ganzheitliche Kriterien wie Systemstabilität und Versorgungssicherheit werden miteinbezogen. Der zentrale Mehrwert liegt in der automatisierten Anpassung von Schutzsystemen an veränderte Netzbedingungen. Dies reduziert den personellen Aufwand signifikant, was insbesondere relevant ist, wenn Schutzparameter durch den schnellen Zubau von erneuerbaren Energien regelmäßig angepasst oder sogar im laufenden Betrieb an neue Betriebszustände angepasst werden müssen (Adaptivschutz). Zusätzlich können durch die ganzheitliche Bewertung der Schutzparameter Fehlkonfigurationen vermieden und die Systemstabilität erhöht werden.

Umgang mit Risiko: Die Schutztechnik stellt einen wesentlichen Bestandteil der kritischen Infrastruktur dar, da sie das Stromnetz vor Fehlern und Ausfällen schützt. Daher erscheint der Einsatz eines KI-basierten Algorithmus zur Ermittlung von Schutzparametern zunächst risikobehaftet, insbesondere da der Lösungsweg des Algorithmus stochastische Elemente enthält. Dies kann in Abhängigkeit gewählter Randbedingungen dazu führen, dass der Algorithmus für jeden Durchlauf andere Lösungen ermittelt. Das Risiko kann jedoch durch den etablierten Prozess der Schutzparameterprüfung deutlich minimiert werden. In dieser Prüfphase werden Fehler im gesamten Netz simuliert, um zu überprüfen, ob die Schutzgeräte korrekt auslösen.

Integration in Infrastruktur: Das System kann offline angewendet werden. Sobald neue Parameter errechnet werden können diese auf bestehende Schutzgeräte überspielt werden. Dies kann vor Ort oder perspektivisch via IEC61850 auch direkt aus der Leitwarte passieren.

Fazit: Trotz der direkten Interaktion mit kritischer Infrastruktur kann für die Schutzparameteroptimierung ein KI-System eingesetzt werden, da Tests bestehen, welche die Ergebnisse in Form von Schutzparametern sehr gut verifizieren können. Die Ergebnisqualität hängt dabei stark von der Bewertungsfunktion ab. In dieser können netzbetreiberspezifische Anforderungen abgebildet werden [28], [29], [30].

Zentrale Kurzschlussortung (post mortem)

Beschreibung & Mehrwert: KI-Verfahren, die komplexe Muster lernen und entdecken, können zur zentralen Kurzschlussortung eingesetzt werden. Zunächst ist ein Einsatz in zeitunkritischen Anwendungen möglich, um z. B. das Betriebspersonal zu unterstützen. Es wäre denkbar solche Methoden direkt in der Ortsnetzstation einzusetzen, um die Reaktionszeiten des Betriebspersonals zu reduzieren und in Kombination mit automatisierten Systemen die Auswirkungen eines Kurzschlusses weiter zu minimieren.

Umgang mit Risiko: Im Labor werden zur Generierung synthetischer Trainingsdaten eine Vielzahl von Szenarien in einem Netzberechnungsprogramm simuliert. Zum Training werden nur die für Schutzsys-

teme üblichen Leiter-Erd-Spannungen und Leiterströme als Eingangsgrößen verwendet. Ausgangsgrößen sind Kurzschlussort und Kurzschlussstrom. Bereits während des Trainingsprozesses stehen Kennwerte zur Verfügung, um die Methode zu bewerten und gegebenenfalls die Trainingsdaten zu erweitern. Nach dieser rechenintensive Trainingsphase kann das KI-Modell, als unveränderliches Modell mit deutlich geringerem Hardwareaufwand, im online Betrieb eingesetzt werden. Die Überprüfung der Modelle kann außerdem in einer klassischen Prüfumgebung mit Sekundärprüfeinrichtungen erfolgen. Alternativ kann die Prüfung in einer virtuellen Prüfumgebung durchgeführt werden. Eine Begrenzung der Anzahl von Messorten ist hier nicht gegeben.

Integration in Infrastruktur: Eine mögliche Integration kann, sowohl in virtuellen Umgebungen (auf zentralen Servereinheiten), als auch auf dezentralen Hardwarekomponenten (Edge-Computing), z.B. in der Ortsnetzstation erfolgen.

Fazit: Die KI-basierte zentrale Kurzschlussortung kann bereits heute den Netzbetrieb bzgl. einer effizienten „post mortem" Fehlerdetektion und Fehlerbehebung unterstützen. Heute übliche Mess- und Verarbeitungssysteme können weiterhin eingesetzt werden. Weiterführende Literatur: [31].

4 Vertrauen schaffen durch einen Implementierungs-prozess

Die vorangegangenen Kapitel betrachteten zwei essenzielle Aspekte für die Einführung von KI: Eine positive Risiko-Nutzen Abschätzung sowie zu erfüllende Rahmenbedingen. Eine dritte wichtige Voraussetzung ist ein zuverlässiger Prozess zur Implementierung – es benötigt Vertrauen in die KI-Nutzung für den spezifischen Anwendungsfall. Dieses Schaffen von Vertrauen muss längerfristig jedoch replizierbar sein, damit KI-gestützte Anwendungen nicht nur in Pilotprojekten genutzt werden, sondern in der Breite der Netzleittechnik. Zentrale Hürden stellen die hohe Komplexität von KI, die benötigten Ressourcen und Kompetenzen, sowie die unscharfe Definition von abstrakten Konzepten wie zum Beispiel Transparenz, Nachvollziehbarkeit und Erklärbarkeit. Initiativen wie die Deutsche Normungsroadmap KI [6] versuchen einen Rahmen zu setzen, eine starke Abhängigkeit vom Kontext bleibt jedoch bestehen. Im Folgenden wird ein Ansatz zur Vertrauensbildung vorgeschlagen, der einen allgemeinen Implementierungsprozess ins Zentrum stellt, anstatt sich auf spezifische KI-Methoden zu konzentrieren. Ziel muss es sein, dass eine Implementierung eines Anwendungsfalls entlang dieses Prozesses als vertrauenswürdig erachtet wird.

Der Implementierungsprozess ist in Abbildung 4 schematisch dargestellt und besteht aus den folgende vier Schritten: Die klare Spezifikation eines Anforderungsprofil, die Entwicklung des Modells, die Prüfung des Modells gegen die Spezifikationen und schließlich die Integration in den Betrieb. Hinzukommen ein regelmäßiges Monitoring, um sicherzustellen, dass die gestellten Anforderungen weiterhin ausreichend sind, sowie im Zweifelsfall ein Nachschärfen der Anforderungsprofile während Entwicklung oder Betrieb. Grundsätzlich ist ein solcher Ablauf etablierten Prozessen sehr ähnlich, so zum Beispiel dem Technisches Sicherheitsmanagement (TSM), Information Security Management System (ISMS) nach ISO/IEC 27001 oder der Softwareentwicklung entlang des V-Modells aus ISO 26262-6, um funktionale Sicherheit zu gewährleisten. Die Grundstruktur des Implementierungsprozesses findet sich auch implizit im AI-Act wieder.

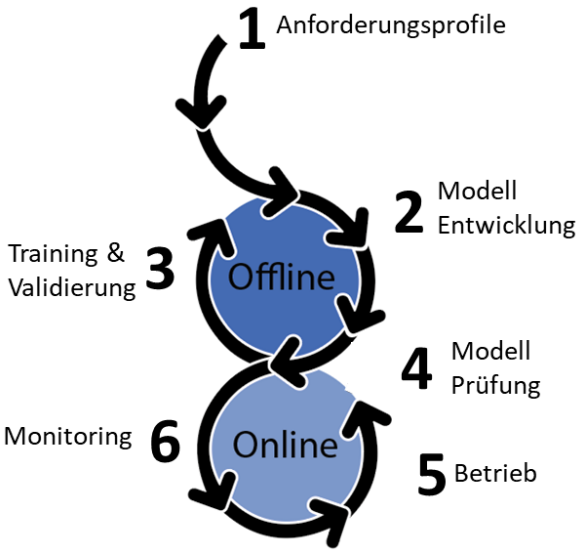

Abbildung 8: Vertrauenswürdiger Implementierungsprozess für Entwicklung eines KI-basierten Modells

Die folgenden Paragrafen stellen die einzelnen Prozessschritte vor:

- **Anforderungsprofil:** Im ersten Schritt müssen die Anforderungen für die Anwendung spezifiziert werden. Diese Spezifikation muss überprüfbar definiert sein – in der Praxis bedeutet dies, dass mit dem Anforderungsprofil nicht nur eine Zielmetrik festgelegt wird, z.B. die Genauigkeit, sondern auch, welche Daten und physikalischen Modelle für die Prüfung eingesetzt werden. Eine erfolgreiche Definition erfordert, dass die Fehlerfolgen hinreichend einbezogen sind. Da die Prüfung vieler KI-basierter Modelle auf statistischen Auswertungen beruht, ist auch die Fehlereintrittswahrscheinlich zu berücksichtigen. Somit geht mit der Erstellung eines Anforderungsprofils eine umfassende Risikobewertung für den Einsatzkontext her. Dies erfordert die Einbeziehung der Kompetenzen von

Modellentwicklern als auch von Anwendern und ist daher nicht nur eine fachliche, sondern auch eine organisatorische Herausforderung. Eine KI-spezifische Möglichkeit zur Modellbewertung bietet die formale Verifikation neuronaler Netze. Im Gegensatz zu herkömmlichen Validierungsverfahren, die meist auf empirischen Tests mit Testdaten basieren, zielt die formale Verifikation darauf ab, bestimmte Eigenschaften des Modells systematisch und beweisbar nachzuweisen [32].

- **Modellentwicklung:** Im nächsten Schritt kann ein KI-gestütztes (oder auch ein konventionelles) Modell entwickelt werden. Dies umfasst typischerweise die Datensammlung und -aufbereitung sowie den Trainingsprozess inklusive eines Validierungsschrittes, um Hyperparameter wie beispielsweise die Modellgröße auszuwählen. Im Trainingsprozess kann eine Vielzahl von Methoden angewendet werden, die wünschenswerte Modelleigenschaften, wie Robustheit oder physikalische Konformität, befördern [33], [34]. Wenn solche Eigenschaften jedoch ein wichtiges Element zur Sicherstellung der Funktionalität darstellen, dann sollte sich dies auch im Anforderungsprofil widerspiegeln. Des Weiteren können Methoden angewendet werden, die die Interpretierbarkeit steigern und gelernte Zusammenhänge aufdecken [35], [36]. Dies kann in der Modellentwicklung helfen, ersetzt jedoch nicht die Modellprüfung.

- **Modellprüfung:** Die Modellprüfung besteht aus einem Abgleich der Spezifikation mit dem entwickelten Modell. Bei Erfüllung aller Kriterien kann das Modell eingesetzt werden, andernfalls muss das Modell verbessert werden oder auch das Anforderungsprofil nachjustiert werden. Letzteres muss jedoch immer im Einklang mit der Risikobewertung stehen. Bei einer erfolgreichen Prüfung wird das Modell und seine Parameter fixiert, es findet also keine Veränderung mehr statt.

- **Betrieb:** Im Betrieb sollte die Funktionalität und die Erfüllung des Anforderungsprofils regelmäßig überprüft werden. Sollte festgestellt werden, dass das Anforderungsprofil nicht mehr zur Betriebssituation passt, muss entschieden werden, ob das KI-basierte Modell weiterhin verwendet werden soll oder nicht. Falls nicht, muss eine Rückfallebene bereitstehen, um einen Weiterbetrieb zu ermöglichen. Weiterhin sind im Rahmen des Monitorings Auffälligkeiten oder unerwünschtes Verhalten des Modells aufzuzeichnen und gegebenenfalls in einer Anpassung der Spezifikation aufzunehmen. Eine bloße Anpassung des Modells auf den spezifischen Ausnahmefall ist nicht ausreichend, da die Prüfkriterien unverändert blieben.

Anhand des Anwendungsfalles „Schutzkonzepte“ aus dem vorherigen Kapitel wird der Implementierungsprozess exemplarisch illustriert und in Bezug zum AI Act gesetzt. Zunächst zum Anforderungsprofil und dessen Überprüfung: Jede Lösung, die das KI-basierte Modell vorschlägt, wird durch eine Reihe von Simulationen überprüft (vgl. Robustheit, Sicherheit und Genauigkeit, Art. 15 AI Act). Diese Simulationen, sowie das zugrundeliegende Netzmodell sind vorab bekannt und durch Experten als hinreichend aussagekräftig zur Bewertung des Schutzkonzeptes bewertet worden (vgl. Qualitätsanforderungen an Trainingsdaten, Art. 10 AI Act). Durch diesen Schritt sind Fragen der Genauigkeit des rechenbaren Schutz- und Netzmodells, der Zuverlässigkeit der Metriken und Bewertung oder die Repräsentativität der ausgewählten Simulationen entkoppelt von der Wahl des zu entwickelnden KI-Modells. Zudem ist auch implizit die Datengrundlage genau definiert. Die Wahl der KI-Methode und ihr Training sind nun nahezu beliebig, solange sich die ausgegebenen Werte überprüfen lassen – im Beispiel wurde eine Particle Swarm Optimization (PSO) gewählt. Erfüllen die vorgeschlagenen Schutzparameter alle Anforderungen und verbessern auch die Güte, könnten sie eingespielt werden und somit ins Feld gebracht werden. Nach der Prüfung geschieht kein weiteres Lernen mehr, das heißt, alle Parameter sind deterministisch festgelegt und Ausgaben überprüfbar. Sollte im Betrieb, beispielsweise durch eine Menschliche Aufsicht (vgl. Menschliche Aufsicht, Art. 14 AI Act), festgestellt werden, dass die Rahmenbedingungen sich im Vergleich zur Spezifikation geändert haben, dann muss dies zur Folge haben, dass die Modellanforderungen an die Rahmenbedingungen angepasst werden. Das zuvor trainierte Modell kann dann auf die erneuerten Anforderungen hin überprüft werden.

Zusammenfassend zeigt sich, dass KI-basierte Modelle entlang des vorgestellten Implementierungsprozesses vertrauenswürdig und funktional sicher entwickelt werden können. Hierbei besteht eine große Ähnlichkeit zu existierenden Implementierungsansätzen von nicht-KI-basierten Modellen. Dies eröffnet die Möglichkeit bestehendes Wissen und etablierte Abläufe zu nutzen, um KI-basierte Methoden praktisch umzusetzen. Die zentrale Schwierigkeit liegt in der Formulierung des Anforderungsprofils. Unvollständige oder unzureichende Spezifikationen führen im weiteren Ablauf leicht zu nicht verifizierbaren oder falsifizierbaren Aussagen sowie zu unklaren Maßstäben, die anfällig für Verzerrungen (Biases) sind. Somit kommt der Definition von nützlichen Anforderungsprofilen eine herausgehobene Bedeutung zu. Diese Aufgabe muss bei der Beschäftigung mit KI von Beginn an berücksichtigt werden und sollte in die strategische Planung der Netzleittechnik einfließen.

5 Zusammenfassung und Ausblick

Die Einführung von KI in der Netzleittechnik ist kein Selbstzweck. **Potenziale** für viele Anwendungsfälle, sowie bereits in der Praxis eingesetzte Methoden werden in diesem Dokument dargestellt. Ein großer Nutzen ergibt sich häufig nicht nur aus der Automatisierung ohne menschliche Eingriffe, sondern auch aus der „Vorbereitung" von Entscheidungen, welche auf vielen Daten basieren.

Jedoch besteht zurzeit das **Risiko einer Überregulierung.** Gleichzeitig ist die Regulierung, speziell der EU AI Act, teils nicht ausreichend konkret, sodass die Erfüllung der Anforderungen schwer überprüfbar ist.

Daher erscheint es sinnvoll in den direkten **Austausch mit entsprechenden Regulierungsorganen** zu gehen und einen vertrauensstiftenden, stufenweisen Implementierungsprozess zu etablieren. Ein Kernpunkt dieses Papiers ist unser **Vorschlag wie ein solcher Implementierungsprozess** in Anlehnung an etablierte Prozesse aussehen könnte. Letztendlich soll dieser Prozess das nötige Vertrauen schaffen, unabhängig von der formalen Prüfung einer KI-Methode.

Wichtige Voraussetzung für den Einsatz dieses Prozesses ist eine klare **Definition der Anforderungen** durch die zukünftigen Betreiber dieser KI-Systeme, beispielweise:

- Was ist der Betriebsbereich? Werden Randbereiche einbezogen?
- Was sind aussagekräftige Metriken, die in der Überprüfung eingesetzt werden?
- Welche Güte muss erreicht werden?

Allerdings stellt die Formulierung überprüfbarer Anforderungen eine zentrale Herausforderung dar. Wenn Anforderungen nur unzureichend formuliert sind oder nicht realistisch überprüft werden können, entsteht ein **Vertrauensproblem** – nicht nur gegenüber der KI, sondern gegenüber dem gesamten System, das auf diesen Anforderungen basiert.

Als besonders geeignet stechen Anwendungsfälle hervor, für die entweder gut **verifizierbare** KI-Methoden eingesetzt werden können, oder bei denen die **Folgen eines Fehlers als eher gering** eingeschätzt werden können. Wenn in einem sehr begrenzten Bereich in der Niederspannung ein Versorgungsausfall durch eine nicht korrekte Funktion entsteht, dann ist das ähnlich zu werten wie ein Kabelschaden durch Baggerarbeiten. Es ist jedoch unerlässlich, über einen Prozess zu verfügen, mit dem in begrenzter Zeit die Versorgung wieder hergestellt werden kann.

Bei der Auswahl eines solchen Anwendungsfalls unterstützt unsere **Darstellung potenzieller Anwendungsfälle und ihrer Risiken**. Der antizipierte Mehrwert einer solchen Anwendung sollte ebenfalls berücksichtigt werden, steht aber bei der Auswahl der ersten einzuführenden Methode nicht im Vordergrund. Der Fokus liegt darauf, zunächst Erfahrung mit dem Implementierungsprozess zu erlangen. Gerade bei Aufgaben, die grundsätzlich gelöst sind, wo jedoch Verbesserungspotenzial erkennbar ist, lässt sich die klassische Methode gut als Benchmark für eine einzuführende KI-Methode nutzen.

Bei jeder KI-Funktionalität besteht wie bei bisherigen Automatisierungsansätzen die Frage, in welchem Verhältnis stehen Kosten und Nutzen der angestrebten Lösung zueinander und wird der Nutzen nicht durch zu viel bürokratischen Aufwand verzehrt bzw. ins Gegenteil verkehrt.
KI-Lösungen sollten nur dann implementiert werden, wenn der Nutzen die identifizierten Risiken klar überwiegt. Hierfür eignen sich insbesondere KI-Systeme, die nicht in einem geschlossenen Regelkreis betrieben werden, sondern lediglich zur Optimierung oder als Entscheidungshilfe dienen. **Qualifiziertes Personal sollte weiterhin die finale Entscheidung treffen.** Die Ergebnisse dieses Schritts sind umfassend zu dokumentieren und notwendige Anpassungen zu begründen. Die setzt jedoch auch voraus, dass das qualifizierte Personal die Bewertungskompetenz haben muss.

Grundsätzlich sollte bei der Einführung von KI-Methoden bedacht werden, dass in der **Vergangenheit bereits häufiger neue Methoden zur Entscheidungsunterstützung** oder gar Automatisierung eingeführt wurden, beispielsweise im Bereich der Optimierung. In diesem Sinne kann bei der Einführung von KI-Methoden ähnlich vorgegangen werden.

Verweise

[1] M. Braun *u. a.*, „Systematisierung der Autonomiestufen in der Netzbetriebsführung“, gehalten auf der Energietechnische Gesellschaft (ETG Kongress) 2021, 2021. Zugegriffen: 19. März 2025. [Online]. Verfügbar unter: https://publica.fraunhofer.de/handle/publica/417067

[2] International Council on Large Electric Systems, Hrsg., *The impact of the growing use of machine learning/artificial intelligence in the operation and control of power networks from an operational perspective.* in Technical brochure / CIGRE, no. 946. Paris, France: CIGRE, 2024.

[3] „Der Digitale Zwilling in der Netz- und Elektrizitätswirtschaft“, VDE ETG, Mai 2023. Zugegriffen: 29. April 2025. [Online]. Verfügbar unter: https://www.vde.com/resource/blob/2257516/cce-234dea484fc0b1943774391752d8a/vde-studie-digitaler-zwilling-data.pdf

[4] European Technology And Innovation Platform For Smart Networks For Energy Transition (Etip Snet), „Unlocking the Potential of AI and Generative AI in European Smart Grids“, European Comission, Apr. 2025.

[5] C. Wendehorst, B. Nessler, A. Aufreiter, und G. Aichinger, „Der Begriff des ‚KI-Systems‘ unter der neuen KI-VO: Vorschlag eines ‚Drei-Faktor-Ansatzes‘ zur Beseitigung von juristischen und technischen Ungereimtheiten“, *MMR - Z. Für IT-Recht Digit.*, Nr. 7, S. 605–614, Juli 2024.

[6] DIN und DKE, „Deutsche Normungsroadmap Künstliche Intelligenz (Ausgabe 2)“, 2022. [Online]. Verfügbar unter: www.din.de/go/normungsroadmapki

[7] L. Kratochwill, P. Richard, L. Babilon, F. Rehmann, S. Mamel, und S. Fasbender, „dena-Analyse. Künstliche Intelligenz - vom Hype zur energiewirtschaftlichen Realität“, 2020, Zugegriffen: 7. März 2025. [Online]. Verfügbar unter: https://publica.fraunhofer.de/handle/publica/300415

[8] „EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act“. Zugegriffen: 15. Juli 2025. [Online]. Verfügbar unter: https://artificialintelligenceact.eu/

[9] „Künstliche Intelligenz für die Energiewirtschaft“, BDEW Bundesverband der Energie- und Wasserwirtschaft, 2020.

[10] B. O. Abisoye, Y. Sun, und W. Zenghui, „A survey of artificial intelligence methods for renewable energy forecasting: Methodologies and insights“, *Renew. Energy Focus,* Bd. 48, S. 100529, März 2024, doi: 10.1016/j.ref.2023.100529.

[11] W. Shin, J. Han, und W. Rhee, „AI-assistance for predictive maintenance of renewable energy systems“, *Energy,* Bd. 221, S. 119775, Apr. 2021, doi: 10.1016/j.energy.2021.119775.

[12] Y. Liu, D. Liu, X. Huang, und C. Li, „Insulator defect detection with deep learning: A survey“, *IET Gener. Transm. Distrib.*, Bd. 17, Nr. 16, S. 3541–3558, Aug. 2023, doi: 10.1049/gtd2.12916.

[13] „Amprion kontrolliert Freileitung mit Drohne“. Zugegriffen: 29. April 2025. [Online]. Verfügbar unter: https://www.amprion.net/Presse/Presse-Detailseite_30144.html

[14] J. R. Andrade *u. a.,* „Data-Driven Anomaly Detection and Event Log Profiling of SCADA Alarms“, *IEEE Access,* Bd. 10, S. 73758–73773, 2022, doi: 10.1109/ACCESS.2022.3190398.

[15] Siemens AG Österreich, „Prozessanomalien frühzeitig erkennen“, Prozessanomalien frühzeitig erkennen.

[16] K. Viereck, A. Saveliev, J. Massmann, und J. Veit, „Results of Long-Term Monitoring for the Proof of Stability in the Switching Process of On-Load Tap-Changers based on Vibroacoustic Measurements“, *Proc CIGRE Sess.,* 2024, Zugegriffen: 29. April 2025. [Online]. Verfügbar unter: https://www.e-cigre.org/publications/detail/a2-11034-2024-results-of-long-term-monitoring-for-the-proof-of-stability-in-the-switching-process-of-on-load-tap-changers-based-on-vibroacoustic-measurements.html

[17] „Assessing potential future artificial intelligence risks, benefits and policy imperatives“, OECD Artificial Intelligence Papers 27, Nov. 2024. doi: 10.1787/3f4e3dfb-en.

[18] M. N. Akhter, S. Mekhilef, H. Mokhlis, und N. Mohamed Shah, „Review on forecasting of photovoltaic power generation based on machine learning and metaheuristic techniques“, *IET Renew. Power Gener.,* Bd. 13, Nr. 7, S. 1009–1023, 2019, doi: 10.1049/iet-rpg.2018.5649.

[19] A. Ghaderi, H. L. Ginn, und H. A. Mohammadpour, „High impedance fault detection: A review“, *Electr. Power Syst. Res.,* Bd. 143, S. 376–388, Feb. 2017, doi: 10.1016/j.epsr.2016.10.021.

[20] J. Lammering *u. a.,* „Detection of Abnormal System- and Operating Behaviour in the Electrical Grid Operation Based on Industrially Proven AI Technology“, in *ETG Congress 2023,* Mai 2023, S. 1–6. Zugegriffen: 12. Juni 2025. [Online]. Verfügbar unter: https://ieeexplore.ieee.org/document/10172977

[21] A. J. Wilson *u. a.,* „The Grid Event Signature Library: An Open-Access Repository of Power System Measurement Signatures“, *IEEE Access,* Bd. 12, S. 76207–76218, 2024, doi: 10.1109/ACCESS.2024.3404886.

[22] „Wie KI potenzielle Gefahren für das Stromnetz frühzeitig erkennen kann“. Zugegriffen: 7. März 2025. [Online]. Verfügbar unter: https://www.psi.de/trends/artikel/wie-ki-potenzielle-gefahren-fuer-das-stromnetz-fruehzeitig-erkennen-kann

[23] „Our Cybersecurity Platform Protects OT Environments | Dragos“. Zugegriffen: 7. März 2025. [Online]. Verfügbar unter: https://www.dragos.com/cybersecurity-platform/

[24] A. M. Prostejovsky, C. Brosinsky, K. Heussen, D. Westermann, J. Kreusel, und M. Marinelli, „The future role of human operators in highly automated electric power systems“, *Electr. Power Syst. Res.,* Bd. 175, S. 105883, Okt. 2019, doi: 10.1016/j.epsr.2019.105883.

[25] „LangChain“. Zugegriffen: 7. März 2025. [Online]. Verfügbar unter: https://www.langchain.com/

[26] „OpenGPT-X: Teuken-7B - Fraunhofer IAIS“, Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS. Zugegriffen: 7. März 2025. [Online]. Verfügbar unter: https://www.iais.fraunhofer.de/de/geschaeftsfelder/speech-technologies/conversational-ai/opengpt-x.html

[27] „GridAnalysis – KI-basierte Systemanalyse von Stromverteilnetzen im Normal- und Kurzschlussbetrieb“. Zugegriffen: 7. März 2025. [Online]. Verfügbar unter: http://gridanalysis.de/

[28] G. J. Meyer, „Protection Concept Optimization Regarding Dynamic Security and Dependability in Multivariate Power Systems“, FAU University Press, Erlangen, 2023. doi: 10.25593/978-3-96147-710-4.

[29] G. J. Meyer *u. a.,* „Digital System Protection Design – A new Toolchain for Protection System Automation“, 3. Juni 2019, *AIM.* doi: 10.34890/906.

[30] G. J. Meyer, J. Jaeger, L. Shang-Jaeger, C. Romeis, und M. Dauer, „Protection Toolchain, Automated Generation of Adaptive Grid Protection Concepts“, 2021, *IEEE.* doi: 10.17023/NR0Q-DY63.

[31] A. Scheidler, „Impact of manual fault location strategies, remote fault indicators and remote switches on system reliability“, gehalten auf der PowerTech, Kiel, 2025.

[32] S. Chevalier, „Trustworthy AI and Machine Learning Verification for Power Systems“, gehalten auf der PSCC 2024, Paris, France, 2024. [Online]. Verfügbar unter: http://www.chatziva.com/PSCC2024Tutorial/2_PSCC2024_Tutorial_Chevalier.pdf

[33] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, und A. Vladu, „Towards Deep Learning Models Resistant to Adversarial Attacks“, gehalten auf der International Conference on Learning Representations, Feb. 2018. Zugegriffen: 6. Mai 2025. [Online]. Verfügbar unter: https://openreview.net/forum?id=rJzIBfZAb

[34] B. Huang und J. Wang, „Applications of Physics-Informed Neural Networks in Power Systems - A Review“, *IEEE Trans. Power Syst.,* Bd. 38, Nr. 1, S. 572–588, Jan. 2023, doi: 10.1109/TPWRS.2022.3162473.

[35] A. Adadi und M. Berrada, „Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)“, *IEEE Access,* Bd. 6, S. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.

[36] R. Machlev *u. a.,* „Explainable Artificial Intelligence (XAI) techniques for energy and power systems: Review, challenges and opportunities“, *Energy AI,* Bd. 9, S. 100169, Aug. 2022, doi: 10.1016/j.egyai.2022.100169.

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Energietechnische Gesellschaft (ETG)

Merianstraße 28
63069 Offenbach am Main
Tel. +49 69 6308-346
etg@vde.com

VDE