Fraunhofer IEE

Gutachten inklusive Implementierungsleitfaden für innovative Anwendungen

Datenanalysen und Künstliche Intelligenz im Stromverteilernetz

Impressum

Herausgeber

Fraunhofer IEE
Fraunhofer-Institut für Energiewirtschaft und Energiesystemtechnik

Joseph-Beuys-Straße 8
34117 Kassel

www.iee.fraunhofer.de

Autorinnen und Autoren:

Kristina Jurczyk
Dr. Sebastian Wende-von Berg
Dr. Kurt Brendlinger

Bildnachweis:

ktsdesign | stock.adobe.com

Stand:

August/2022

Inhalt

Executive Summary

Das Energiesystem befindet sich im Wandel, maßgeblich geprägt durch die Einflüsse und Auswirkungen der Energiewende. Der Umstieg von fossilen Brennstoffen auf erneuerbare Energien stellt neue Herausforderungen sowie Anforderungen an die Stromnetze, wie z.B. die Integration von dezentralen, volatilen Erzeugungsanlagen und flexiblen Lasten. Hinzu kommt die fortschreitende Digitalisierung, die auch die Energiewirtschaft beeinflusst und neue Möglichkeiten in Bezug auf datenbasierte und datengetriebene Anwendungen liefert, aber auch Herausforderungen in Bezug auf Datensicherheit und -abhängigkeit für Netzbetreiber mit sich bringt. Um die steigende Komplexität beherrschen zu können, müssen Prozesse effizienter gestaltet und innovative Konzepte genutzt werden. Digitalisierung kann hier helfen, indem z.B. die extrem große Anzahl an kleinen erneuerbaren Erzeugern aber auch flexiblen Lasten durch permanente Kommunikationsanbindungen durchgängig in Echtzeit gesteuert und somit koordiniert werden könnten. Einen vielversprechenden Ansatz bieten Methoden der Künstlichen Intelligenz (KI), die bereits in vielen Bereichen erfolgreich eingesetzt und genutzt werden. „KI bildet derzeit die Speerspitze der Digitalisierung, weil durch KI zahlreiche kognitive Leistungen, die bislang nur mit menschlicher Intelligenz erbracht werden konnten, erstmals automatisierbar werden“ [43].

In dem dena-Projekt Data4Grid wird der Nutzen von Datenanalysen und Künstlicher Intelligenz in Stromnetzen untersucht. Dabei sollen Bereiche identifiziert werden, in denen innovative Anwendungen zukünftig einen Mehrwert für Netzbetreiber bieten können. Das Projekt gliedert sich in zwei Teile. Beide Teile wurden von einem Verteilnetzbetreiber-Gremium begleitet, das sich aus 14 deutschen Verteilnetzbetreibern verschiedener Größe zusammensetzt, die unterschiedliche Erfahrungen mit dem Einsatz von Datenanalysen und KI aufweisen. In einem praktischen Teil wurden in Form von Challenges drei ausgewählte Anwendungsfälle bearbeitet, die den praktischen Nutzen von innovativen Anwendungen demonstrieren sollen. Ergänzt wird der praktische Teil durch dieses, hier vorliegende, wissenschaftliche Gutachten, das sich insbesondere mit den Veränderungen und der Digitalisierung der Stromverteilernetze befasst.

Die Stromversorgung ist als kritische Infrastruktur besonders zu schützen, weshalb der Einsatz von neuen Anwendungen wie Datenanalysen und KI vor ihrer Einführung in den Netzbetrieb besonderer Vorsicht bedarf. Im Gutachten werden u.a. die Fragen diskutiert, ob der Einsatz von innovativen Anwendungen zu neuen kritischen Prozessen führen kann oder ob diese dabei helfen können die Kritikalität einzelner Prozesse abzuschwächen. Haben KI-Methoden zukünftig eine Schlüsselfunktion im Stromnetz oder ist es riskant künstliche Intelligenz in einem so kritischen Bereich einzusetzen? In Kapitel 2 wurden daher die Prozesse in der kritischen Infrastruktur der Stromnetze und deren Betreiber betrachtet sowie auf die Nutzung von datengetriebenen Prozessen mit Fokus auf die Verwendung von künstlicher Intelligenz und deren Risiken eingegangen. Ein primäres Risiko ist hierbei die gegenseitige Abhängigkeit des Stromnetzes und dessen Datenproduktion von der Informations- und Kommunikationstechnologie (IKT). Ein fehlerhafter oder abgebrochener Prozess in einem der beiden Felder kann zu direkten Konsequenzen im jeweils anderen Feld führen, weshalb die datenabhängigen Prozesse bzw. ihre genutzten Anwendungen kritisch geprüft und auf ihren Einfluss hin charakterisiert werden sollten. Um die Kritikalität neuer Prozesse und Anwendungen in den verschiedenen Bereichen des Netzbetriebs einzuordnen,

wurden Indikatoren definiert. Prozesse, die im Umfeld der Netzbetriebsführung und operativen Planung sowie der IKT-Sicherheit mit hoher Systemrelevanz und potenzieller IKT- und Datengefährdung stattfinden, besitzen das größte Gefahrenpotential und werden als potenziell kritisch eingeordnet. Prozesse im Bereich der Instandhaltung und dem Endkundenbereich sind in der Regel weniger kritisch, da ihre unmittelbaren Auswirkungen deutlich geringer sind. Ebenfalls wurden KI-Anwendungen auf potenzielle neue Risiken hin diskutiert. Hier wurden insbesondere die Abhängigkeit von der Datengrundlage sowie ein möglicherweise entstehendes zu hohes Vertrauen in die Ergebnisse der KI und die oft fehlenden Möglichkeiten die Ergebnisse nachzuvollziehen identifiziert. Letzteres liegt einerseits oftmals an dem Black-Box Charakter der KI-Anwendungen, aber auch daran, dass Menschen die Entscheidungen der KI nicht mehr rational nachvollziehen können.

Eine wesentliche Voraussetzung für den gesicherten Ablauf kritischer Prozesse und die Koordination zwischen den Akteuren im Energiesystem ist ein effizienter Informationsaustausch in Form von verschiedensten Daten. In diesem Zusammenhang werden die verschiedenen Prozesse der Datenwertschöpfungskette untersucht, die von der Datenerfassung über die Datenübertragung bis hin zur Anwendung reichen. Dabei erfolgt u.a. die Einordnung der aktuellen Datenverfügbarkeit bei Verteilnetzbetreibern sowie die Betrachtung von Risiken, die bei der Datennutzung entstehen können. In Kapitel 3 werden daher die Daten an sich betrachtet und ihre Erfassung, Verfügbarkeit und Qualität diskutiert. Weiterhin wird auf mögliche datenbasierte Risiken, wieder mit Bezug zu datengetriebenen Prozessen und dem Einsatz künstlicher Intelligenz, hingewiesen. Als primäre Erkenntnisse sind hier zu nennen, dass eine automatisierte Datenerfassung und Archivierung die Grundlage für eine erfolgreiche Digitalisierung der eigenen Prozesse bilden kann. Weiterhin wird ein deutlicher Mehrwert in dem Verschneiden und Korrelieren von internen und externen Daten gesehen, da dadurch ein signifikanter Erkenntnisgewinn erzielt werden kann (z.B. Messzeitreihen mit Wetterdaten korrelieren). Bei der Evaluation von verfügbaren Datenquellen fällt auf, dass ein Großteil nicht öffentlich verfügbar ist und eine fehlende Open-Data Mentalität im Bereich der Energieversorgung zu erkennen ist. Weiterhin fiel auf, dass unterschiedliche Datenformate und Standards eine Vergleichbarkeit der Daten untereinander und den direkten Einsatz erschweren. Abschließend wird auch noch auf das Halten und Nutzen von z.T. sensiblen Daten eingegangen. Hier liegt die Verantwortung beim Datenhalter und dieser muss sicherstellen, dass seine Daten vor unerlaubten Zugriffen oder Manipulationen geschützt sind. Die Nutzung von aktuellen Verschlüsselungsverfahren und weiteren Schutzmaßnahmen ist unerlässlich.

Weiterhin erfordert eine datengetriebene Energiewirtschaft mit vielen untereinander vernetzen Akteuren einen klar definierten regulatorischen Rahmen. Hierzu zählen sowohl Regelungen im energiewirtschaftlichen Kontext als auch primär der regulatorische Rahmen für den Umgang mit Daten. Auch spezielle Vorgaben für den Einsatz von KI-Methoden werden aktuell viel diskutiert, um einen einheitlichen Rahmen für deren Nutzung zu schaffen. Die wichtigsten regulatorischen Rahmenbedingungen werden in diesem Gutachten kurz in Kapitel 4 erläutert. Es wurde festgestellt, dass die aktuellen gesetzlichen und regulatorischen Rahmenbedingungen keine unüberwindbaren Hürden für den Einsatz datengetriebener Prozesse und KI-Anwendungen darstellen. Der entstehende Aufwand durch Beachtung der Rahmenbedingungen oder durch die Einführung

eines ISMS nach ISO27000 kann aber dazu führen, dass neue Prozesse und Anwendungen nicht eingeführt werden und es zu einem Innovationsstau kommen kann.

Abschließend wurden im Rahmen der Gutachtenerstellung zwei Workshops mit den am Projekt Data4Grid teilnehmenden Verteilnetzbetreibern durchgeführt, bei denen der Einsatz von Datenanalysen und KI im Stromnetz im Fokus standen. Hierbei wurden u.a. kritische Prozesse im Stromnetz diskutiert, Schwierigkeiten hinsichtlich der Datenerfassung und Datenbereitstellung sowie Hürden bei der Einführung innovativer Technologien. Während der Diskussionen kristallisierte sich der Wunsch der Netzbetreiber nach einem Leitfaden bzw. Richtlinien für die Einführung innovativer Anwendungen heraus, da viele Netzbetreiber trotz der großen Anwendungsbreite vor der Frage stehen, ob sich die Einführung digitaler Prozesse und damit möglicher datengetriebener (KI-)Anwendungen überhaupt lohnt und womit bei einer konkreten Umsetzung begonnen werden muss.

Um Netzbetreiber bei dieser Aufgabe zu unterstützen und die Einführung von datengetriebenen innovativen Anwendungen zu vereinfachen sowie deren mögliche Risiken zu minimieren, wurde neben den beschriebenen Kernelementen des wissenschaftlichen Gutachtens ein Implementierungsleitfaden entwickelt (Kapitel 5). Dieser bildet die wesentlichen Schritte und Überlegungen ab, die über die verschiedenen Phasen einer Einführung von Datenanalysen im Unternehmen relevant sind. Das sind Entscheidungspfade, Machbarkeitsanalyse und Mehrwert, Planung, Durchführung, Test und Validierung, Inbetriebnahme und abschließend Wartung und Weiterentwicklung. Als konkrete Beispiele wurden drei Anwendungen anhand des Leitfadens analysiert.

Zusammenfassend lässt sich sagen, dass die deutschen Verteilnetzbetreiber vor einer großen Aufgabe stehen. Wenn die Digitalisierung und Automatisierung einen Mehrwert für den Betrieb der Stromnetze liefern soll, dann gehören datengetriebene Prozesse und KI-Anwendungen mit dazu. Die angesprochenen Herausforderungen und Risiken stellen keine unüberwindbaren Hindernisse da und sollten frühzeitig angegangen werden. Hierzu gehört auch schon heute die Datengrundlage für morgen zu legen. Verteilnetzbetreiber sollten sich proaktiv in die digitale Transformation begeben. Dazu gehört auch eine Mentalität der Agilität, d.h. neues auszuprobieren.

1 Welche Herausforderungen gilt es im heutigen und zukünftigen Stromnetz zu meistern?

Daten sind das neue (Schmier-)Öl im Getriebe der Energiewende und treiben diese an.

> *Dieser Eindruck kann schnell durch die gewaltige Flut an Informationen entstehen, die zum einen jeden Tag generiert, zum anderen aber auch bereits benötigt werden. Smart Meter sollen Transparenz in die Niederspannung bringen und Ladepunkte zusammen mit E-Kfz könnten, bei der richtigen Koordination, dafür sorgen, dass Überschüsse an Energie aus volatiler erneuerbarer Erzeugung bedarfsgerecht aufgenommen werden können. Daten gelten, neben den erneuerbaren Energien, als Schlüssel der Energiewende für den Umstieg von fossilen Brennstoffen auf eine nachhaltige Energieversorgung. Das zeigt auch der 2021 eingeführte Redispatch 2.0 – Prozess, bei dem große Mengen an Information viertelstündlich ausgetauscht und aktualisiert werden müssen, damit die Koordination von Flexibilitäten über mehrere Spannungsebenen reibungslos funktioniert und Engpässe zielgenauer und effektiver bearbeitet werden können ohne unnötig Energie aus den Erneuerbaren einzusenken und ungenutzt zu lassen.*

Die Struktur des Energieversorgungssystems, das konventionell von wenigen zentralen Großkraftwerken geprägt war, wandelt sich durch die vermehrte Installation von erneuerbaren Energien hin zu einer dezentralen Struktur mit vielen kleinen Erzeugern. Neben dem Ausbau der erneuerbaren Energien nimmt die Erhöhung der Effizienz eine bedeutende Rolle ein. Beide Prozesse stellen neue Anforderungen an die Stromnetze, insbesondere die Stromverteilernetze, die wesentlich von den Veränderungen betroffen sind. Zur Bewerkstelligung der neuen Herausforderungen bedarf es intelligenter Netze, in denen alle Netznutzer miteinander vernetzt sind und in denen digitale Technologien in Verbindung mit innovativen Methoden zum Einsatz kommen. Von besonderem Interesse sind datengetriebene Anwendungen speziell in Verbindung mit Methoden der künstlichen Intelligenz, die einen entscheidenden Beitrag leisten sollen. Dass durch die Verfügbarkeit und Nutzung neuer Daten aus und über das Energiesystem und in der Verwendung innovativer Methoden und Anwendungen nicht nur Potenziale liegen, sondern auch Herausforderungen und sogar Risiken, wird in diesem Gutachten vor dem Hintergrund von Prozessen in einer kritischen Infrastruktur betrachtet und diskutiert.

1.1 Energiewende

Die Energiewirtschaft ist einer der Hauptverursacher von Treibhausgasemissionen, etwa 35 % der Emissionen in Deutschland wurden im Jahr 2020 durch die öffentliche Strom- und Wärmeerzeugung aus fossilen Energieträgern verursacht [2]. Mit dem Bundes-Klimaschutzgesetz (KSG) aus dem Jahr 2021 wurden die Klimaziele der Bundesregierung für Deutschland noch einmal verschärft. Bis zum Jahr 2030 sollen die Treibhausgase um 65% gegenüber 1990 reduziert werden, bis 2040 soll eine Reduktion um 88% erreicht sein, bis 2045 die Treibhausgasneutralität [3]. Ein Kernpunkt für die Dekarbonisierung ist die Nutzung von klimaneutralen Energieträgern, das heißt Strom muss aus erneuerbaren Quellen hergestellt werden. Hierfür muss der Ausbau von Windkraft- und Photovoltaikanlagen weiter vorangetrieben werden [4].

In der Studie „Langfristszenarien für die Transformation des Energiesystems in Deutschland 3“ von Fraunhofer ISI, Consentec, TU Berlin und dem ifeu aus 2021 wurde untersucht wie Deutschland das Ziel der Treibhausgasneutralität erreichen kann [4]. Hierfür wurden drei verschiedene Szenarien zur klimaneutralen Energiegewinnung betrachtet, wobei je ein Szenario mit der intensiven Nutzung von Strom, Wasserstoff und synthetischen Kohlenwasserstoffen modelliert wurde. Eine Gemeinsamkeit aller drei Szenarien ist, dass der gesamte Stromverbrauch zur Erreichung der Ziele in den kommenden Jahren deutlich ansteigt; bis 2050 könnte er sich für Deutschland im Vergleich zu 2020 auf ca. 1000 TWh nahezu verdoppeln [4]. Speziell der Verkehr- und Wärmesektor unterliegen einem grundlegenden Wandel, der signifikante Auswirkungen auf den Strombedarf hat. Verbrennungsmotoren und Heizkessel, die fossile Brennstoffe nutzen, sollen durch den Ausbau der Elektromobilität und die vermehrte Installation von Wärmepumpen sukzessiv abgelöst werden [6]. Bis zum Jahr 2030 soll, laut dem Koalitionsvertrag 2021-2025, die Anzahl von E-Autos auf 15 Mio. steigen, was einem Anteil von ca. 30% entspricht, und 6 Mio. Wärmepumpen sollen installiert sein [5]. Des Weiteren legen aktuelle politische Entwicklungen (2022) nahe, dass zukünftig weniger Gas und Öl und mehr elektrische Energie in Form von Wärmepumpen zum Heizen benutzt wird und somit der Energiebedarf weiter ansteigt.

Basierend auf den Ergebnissen der „Langfristszenarien-Studie“ sowie weiterer Studien wurde im Januar 2022 von den Übertragungsnetzbetreibern (ÜNB) ein Entwurf für den Netzentwicklungsplan Strom für 2037 vorgestellt. Dieser gibt erstmals einen Ausblick auf ein „Klimaneutralistätsnetz 2045“, d.h. ein Stromübertragungsnetz in einem klimaneutralen Deutschland [7]. Neben dem Übertragungsnetz steigen die Anforderungen aber vor allem in den Verteilnetzen in der Mittel- und Niederspannungsebene, weshalb Anpassungen auf allen Spannungsebenen notwendig sind.

Konventionelle Großkraftwerke speisen in das Übertragungsnetz ein, das die Höchstspannungsebene in Deutschland bildet. Der Energiefluss war klassisch aus dem Übertragungsnetz in das Verteilnetz gerichtet, das sich aus der Hoch-, Mittel- und Niederspannung zusammensetzt. Die verschiedenen Spannungsebenen sind über Umspannwerke miteinander verbunden, in denen die Spannung entsprechend transformiert wird. Die Integration von regenerativen Erzeugungsanlagen (EE-Anlagen) stellte die konventionelle Netzinfrastruktur, spätestens seit den 2010er Jahren, vor neue Herausforderungen, denn Erzeugungsanlagen, die erneuerbare Energiequellen zur Stromerzeugung nutzen, speisen vorrangig im Verteilnetz ein [8]. Hinzu kommt eine schwankende Einspeiseleistung von EE-Anlagen aufgrund der Abhängigkeit vom Wetter sowie der Jahres- und Tageszeit, sodass bei übermäßiger Stromproduktion durch regenerative Anlagen überschüssiger Strom aus dem Verteilernetz zurück in das Übertragungsnetz gespeist werden muss. Ein schematischer Aufbau der verschiedenen Spannungsebenen ist in Abbildung 1 dargestellt. Der ursprünglich passive, bezugsorientierte Betrieb der Verteilnetze weicht seit Jahren zunehmend einem aktiven, einspeiseorientierten Betrieb, wodurch sich die Systemführung, die historisch überwiegend auf Ebene des Übertragungsnetzes mit großen fossilen Kraftwerken stattfand, auch auf die Verteilnetze ausweitete. Hier standen, bzgl. eines aktiven Netzbetriebes, neben den Höchst- zuerst die Hochspannungsnetze im Fokus, in denen sich durch direkte Einspeisung und Rückspeisung aus den MS-Netzen vermehrt Engpässe einstellten, was eine weiterhin aktivere und vor allem koordinierte Betriebsführung verlangte.

Ein signifikanter Aspekt dabei ist auch die zeitnahe Abstimmung mit den unter- und überlagerten Netzbetreibern und deren Netzebenen (siehe hierzu auch Redispatch 2.0 [13]). Der Austausch von Informationen in Echtzeit wird zukünftig notwendig werden, um das jetzt schon komplexe, elektrische Energiesystem stabil, robust, zuverlässig und sicher zu betreiben.

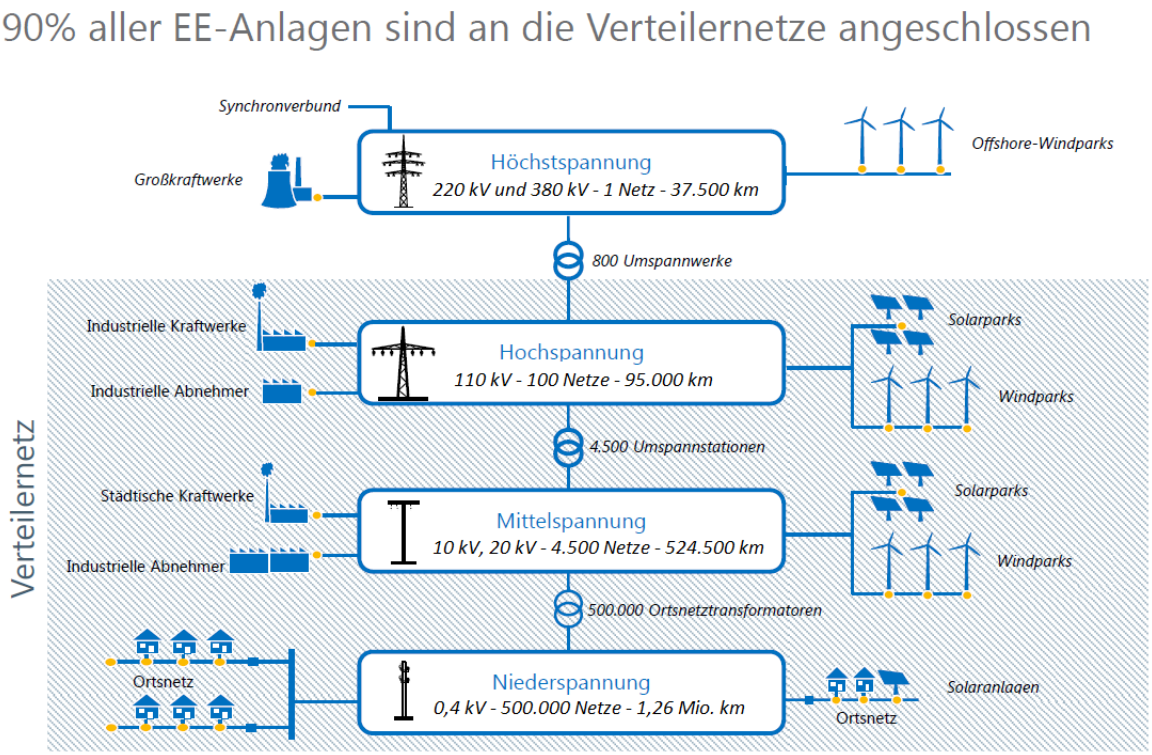


Abbildung 1: Aufbau der verschiedenen Spannungsebenen im deutschen Stromnetz (Quelle: geändert, BMWI Verteilernetzstudie, Plenarsitzung, 2014, S. 6, mit aktualisierten Werten der BNetzA 2021).

1.2 Notwendigkeit für Veränderungen

Durch die dezentrale Verteilung der regenerativen Erzeugungsanlagen, die schwankende Einspeiseleistung und daraus resultierende bidirektionale Leistungsflüsse werden die Stromverteilernetze zunehmend komplexer. Weitere Herausforderungen sind die Integration von E-Autos und Wärmepumpen als flexible Lasten, die auch zur gezielten Einspeisung in das Netz genutzt werden können bzw. Potentiale zur zeitlich variablen Gestaltung der Leistungsbezüge bieten sowie sich zukünftig verändernde Rahmenbedingungen durch Batteriespeicher [7].

Die volatile Erzeugung führt aktuell dazu, dass in einigen Regionen nicht zu jeder Zeit der Strom aus EE-Anlagen vollständig abgenommen und übertragen werden kann, da die Netze noch nicht für solch hohe Einspeisungen in den unteren Spannungsebenen ausgelegt sind. Hierdurch können Grenzwertverletzungen wie thermische Betriebsmittelüberlastungen auftreten [12]. Auch die erhöhte Zahl von Anschlussbegehren für Ladesäulen und Wallboxen für E-Autos kann neue Herausforderungen für Netzbetreiber mit sich bringen. Zum Beispiel können fehlende Beobachtungsmöglichkeiten, aufgrund mangelnder Messstellen in Mittel- und Niederspannungsnetzen, dazu führen, dass Netzbetreiber nicht genau sagen können wie viele neue Wallboxen in einem bestimmten Netzgebiet überhaupt zulässig wären, damit diese bei hoher Gleichzeitigkeit nicht zu

Grenzwertverletzungen wie Engpässen führen. Teilweise sind auch die genauen Standorte von Ladesäulen und Wallboxen unbekannt für den Netzbetreiber, wodurch deren Einbeziehung in Netzausbauplanungen nur grob möglich ist. Um aber daraus drohende, potenzielle Überlastungen an den davon betroffenen Transformatoren erkennen zu können, sind diese Angaben notwendig. Dass die Auslastung der Transformatoren stetig ansteigen wird, wurde bereits durch Szenarien der Langfristszenarien-Studie [4] und den Zielen im Koalitionsvertrag [5] deutlich. In einem potenziellen Störungsfall können benachbarte Transformatoren dann einen ausgefallenen Bereich kaum noch oder auch gar nicht mehr mitversorgen. Aufgrund fehlender Überwachung könnten potenzielle Grenzwertverletzungen dabei nicht bemerkt werden.

Eine mögliche Lösung bieten innovative Konzepte wie regelbare Ortsnetztransformatoren oder Blindleistungsbereitstellung durch Photovoltaik-Wechselrichter, z.B. für eine lokale dynamische Spannungsregelung [15]. Um allerdings aktiv Wirk- und Blindleistung in MS- und NS-Netzen zu steuern, lokale Überlastungen gezielt zu reduzieren oder auch Systemdienstleistungen bereitzustellen, fehlt aktuell noch eine ausreichende Messinfrastruktur, um Betriebsmittelzustände und den gesamten Netzzustand zu beobachten und auf Basis dieser Information Entscheidungen abzuleiten. Im Gegensatz zur Hochspannung müssen hierfür Mittel- und Niederspannungsnetze noch mit einer entsprechenden Technik und Sensorik ausgestattet werden. Aufgrund der Länge und verzweigten Struktur des Verteilnetzes wäre aber eine flächendeckende Einrichtung von Messstellen mit entsprechender Sensorik sehr kosten- und zeitintensiv [14].

> *Um der Komplexität und den steigenden Anforderungen im Verteilnetz gerecht zu werden, ist der Einsatz digitaler Systeme mit einer hochmodernen Dateninfrastruktur in Verbindung mit künstlicher Intelligenz (KI) sehr vielversprechend.*

1.2.1 Digitalisierung

Die Prozesse der Digitalisierung beeinflussen zunehmend fast alle Lebensbereiche unserer Gesellschaft, einen Großteil der Wirtschaft und auch die Energieversorgung. Zusammen mit der Energiewende und ihrer dezentralen und wetterabhängigen Erzeugung aus Windkraft- und PV-Anlagen sowie flexiblen Lasten auf der Verbraucherseite verändert die Digitalisierung den Netzbetrieb und dessen Kommunikationsketten grundlegend [14]. Mehr und mehr Anlagen und Betriebsmittel in den Stromnetzen sind mit moderner, digitaler Kommunikationstechnik ausgestattet und können somit umfänglich in digitalisierte und automatisierte Prozesse eingebunden werden. Insbesondere entstehen dadurch in den Niederspannungsnetzen auch neue Möglichkeiten, u.a. Netzzustände auf Basis der Echtzeitmessdaten von z.B. Smart-Metern, Ladepunkten oder PV-Wechselrichtern zu bestimmen.

Die damit verbundene exponentiell wachsende Datenmenge [43] bringt allerdings auch viele neue Herausforderungen und potenzielle Gefahren mit sich, kann aber auch immense Chancen generieren. Im traditionellen Stromnetz mit konventionellen Kraftwerken war die Einspeisung der großen Kraftwerke planbar. Vor der Energiewende fand primär eine Kommunikation zwischen den Netzleitstellen der ÜNBs, den Großkraftwerken und den Umspannwerken statt. Hierdurch wurde die Frequenz- und Spannungsregelung in der jeweiligen Regelzone gewährleistet. Zukünftig soll die Einbindung aller Netznutzer erfolgen, die sich von steuerbaren Erzeugungsanlagen über steuerbare Speicher bis hin zu regelbaren Kleinstverbrauchern in einzelnen Haushalten

erstreckt. Hierdurch werden Informations- und Kommunikationssysteme (IKT-Systeme) erforderlich, die Millionen dezentrale Teilnehmer verbinden. Die Vernetzung und das steigende Volumen an aussagekräftigen Daten in Verbindung mit neuen Möglichkeiten der Datenauswertung bilden die Grundlage für den Aufbau von intelligenten Netzen (Smart Grids).

Smart Grids

„Der Begriff Smart Grids umfasst, gemäß dem Verband der Elektrotechnik Elektronik Informationstechnik e.V. (VDE), die Vernetzung und Steuerung von intelligenten Erzeugern, Speichern, Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und Verteilernetzen mithilfe von Informations- und Kommunikationstechnologie (IKT), womit auf der Grundlage eines transparenten, energie- und kosteneffizienten sowie sicheren und zuverlässigen Systembetriebs eine nachhaltige und umweltverträgliche Sicherstellung der Energieversorgung gewährleistet werden soll“[12]. Hierfür bedarf es künftig vermehrt dem Einsatz digitaler Technologien, wie Sensoren in Betriebsmitteln und Geräten, Messtechnik im Netz und Software, mit denen die einzelnen Akteure in fast allen Bereichen der energiewirtschaftlichen Wertschöpfungskette (Erzeugung, Transport, Speicherung, Verteilung) miteinander vernetzt werden. Durch ein gesteigertes Monitoring und einer Auswertung dieser Daten in Verbindung mit z.B. Prognosen, besteht dann die Möglichkeit über steuerbare Betriebsmittel in den Netzbetrieb aktiv einzugreifen und somit kann eine verbesserte Netzstabilität und -sicherheit bei gleicher Auslastung erreicht werden sowie eine optimierte Nutzung von bereits bestehenden Flexibilitäten (Höchst- und Hochspannung) und Erschließung neuer Flexibilitäten (Mittel- und Niederspannung). Eine Grundlage für die flächendeckende Ausstattung mit kommunikationsfähiger Hardware wurde mit dem Smart Meter Rollout geschaffen (vgl. Kapitel 3.1.1) [14].

Innovative Technologien, die zur Effizienzsteigerung der Netze beitragen können, unterstützen somit das NOVA-Prinzip, das als Grundlage für die Netzplanung dient: **N**etz**o**ptimierung vor **V**erstärkung vor **A**usbau [9].

> *Um diese Anforderung erfüllen zu können, muss der Aufbau von intelligenten Netzen erfolgen, bei denen datengetriebene Prozesse im Vordergrund stehen.*

1.3 Zusammenfassung und Struktur des Gutachtens

Die stärkere Vernetzung der einzelnen Netzbetreiber ermöglicht bereits branchenweite Lösungen wie den Redispatch 2.0. Die Branchenlösung Redispatch 2.0 wurde 2021/2022 eingeführt, mit dem Ziel „Netzengpässe über alle Netzebenen hinweg unter Einbezug aller wesentlichen Energieanlagen (>100 kW) effizient“ zu beheben [13]. Hiermit wird auf die sich ändernden Anforderungen und Rahmenbedingungen reagiert. Der Redispatch 2.0 ist für alle Netzbetreiber relevant und die Grundlage hierfür bilden Mess- und Prognosedaten sowie der regelmäßige, zeitnahe Austausch dieser Informationen zwischen den Netzbetreibern[14].

> *Neben den vielfältigen Möglichkeiten durch die Nutzung neuer Daten und Informationen entstehen aber auch neue Herausforderungen und Risiken, die im Folgenden detailliert betrachtet werden. Zum Beispiel sind digitalisierte Prozesse in der Netzbetriebsführung stark abhängig von der jeweiligen Datengrundlage und dem kontinuierlichen Strom neuer aktueller Daten. Sind*

> *diese aus verschiedenen Gründen einmal nicht vorhanden, kann es schnell zu kritischen Situationen im Stromnetz kommen, die dann wiederrum die Versorgungssicherheit gefährden können. Auch falsche Interpretation oder Nutzung von Messdaten können zu einer Gefährdung der Netzsicherheit führen.*

Die Verfügbarkeit und Nutzung verschiedener Arten von Daten und Informationen soll in den folgenden Kapiteln vor dem Hintergrund kritischer Prozesse und Rahmenbedingungen der Gesetzgebung im Stromnetz analysiert werden. In Kapitel 2 werden die Prozesse in der kritischen Infrastruktur der Stromnetze und deren Betreiber betrachtet sowie auf die Nutzung von datengetriebenen Prozessen mit Fokus auf die Verwendung von künstlicher Intelligenz und deren Risiken eingegangen. In Kapitel 3 werden die Daten an sich betrachtet und ihre Erfassung, Verfügbarkeit und Qualität diskutiert. Weiterhin wird auf mögliche datenbasierte Risiken, wieder mit Bezug zu datengetriebenen Prozessen und dem Einsatz künstlicher Intelligenz (KI), hingewiesen. In Kapitel 4 wird kurz auf den gesetzlichen regulatorischen Rahmen eigegangen und speziell über Sicherheitsanforderungen mit Fokus auf Daten und KI diskutiert. Kapitel 5 soll dann einen anwendungsnahen Leitfaden über ein mögliches Vorgehen zum Planen, Einrichten und Nutzen datengetriebener KI-basierter Anwendungen und Prozesse geben. Eine Zusammenfassung mit Ausblick wird abschließend in Kapitel 6 beschrieben.

2 Datengetriebene Anwendungen auf Basis künstlicher Intelligenz vor dem Hintergrund kritischer Prozesse im Stromnetz

Mit der voranschreitenden Digitalisierung steigt auch die Anzahl der Möglichkeiten für den Einsatz von Datenanalysen und innovativen datengetriebenen Anwendungen im Stromnetz. Ebenso steigt aber auch die Abhängigkeit von genau diesen Daten sowie von der elektrischen Energie an sich in vielen Bereichen unserer Gesellschaft extrem stark an, wodurch gerade ein Stromausfall oder sogar ein totaler „Blackout" besonders kritisch und gefährlich sein kann. Aber nicht nur ein Stromausfall kann extreme Folgen nach sich ziehen, auch Hackerangriffe, Datenausfälle oder Fehlinterpretation von Daten können zu Versagen von Prozessen und Anwendungen führen und somit ebenfalls die Versorgungssicherheit gefährden.

Vor diesem Hintergrund werden in diesem Kapitel eine Auswahl kritischer Prozesse und der Einfluss von datengetriebenen Anwendungen unter Verwendung künstlicher Intelligenz diskutiert. Ziel ist es, die in den verschiedenen Bereichen des operativen Netzbetriebes stattfindenden kritischen Prozesse zu identifizieren und einordnen zu können. Weiterhin sollen datengetriebene Anwendungen innerhalb dieser Prozesse allgemein auf potenzielle Risiken aber auch Chancen hin evaluiert und speziell der Einsatz von KI diskutiert und bewertet werden. Für einen groben Überblick werden abschließend verschiedene mögliche KI-Anwendungen kurz charakterisiert und deren Mehrwerte herausgestellt.

2.1 Ausfall kritischer Infrastruktur

Kritische Infrastrukturen

Die Stromversorgung in Deutschland gehört zur kritischen Infrastruktur in der Energiewirtschaft (Festlegung vom Bundesamt für Sicherheit in der Informationstechnik, BSI-Kritisverordnung (BSI-KritisV)) [21]. „Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden" [16]. Die Vermeidung und Behebung von kritischen Situationen, zu denen Grenzwertverletzungen wie z.B. Leitungsüberlastungen sowie das Erkennen und Verhindern von Cyber-Attacken auf das Energiesystem und der Ausgleich zwischen Angebot und Nachfrage auf Markt- und Netzebene gehören, zählen zu den Kernaufgaben der Netzbetreiber [11].

Neben der Elektrizität gehören im Sektor Energie die Bereiche Gas, Mineralöl und Fernwärme zu den kritischen Branchen. In diesem Gutachten messen wir der Stromversorgung als kritische Branche eine besondere Bedeutung bei, da nicht nur andere kritische Infrastrukturen wie der Verkehr oder die medizinische Versorgung von ihr abhängen, sondern auch insbesondere die gesamte Kommunikationsinfrastruktur in Deutschland aber auch weltweit, von elektrischer Energie abhängig ist und diese in der Regel zentral und nicht lokal bereitgestellt wird. Diese Abhängigkeit reicht mittlerweile nicht nur durch Smart Homes, sondern durch den täglichen Informationsbedarf

auch weit in den privaten Bereich hinein und verdeutlicht die allgegenwärtige Abhängigkeit und Verletzlichkeit dieser Infrastruktur bei Versorgungsausfällen [16]. Ein weiterer kritischer Sektor wird von der Informations- und Kommunikationstechnologie (IKT) gebildet, der ebenfalls unverzichtbar für Staat, Wirtschaft und Gesellschaft ist. „Die Informationstechnik und Telekommunikation umfassen die Sprach- und Datenübertragung sowie die Datenspeicherung und Datenverarbeitung [16]".

> *Mit der zunehmenden Digitalisierung und Vernetzung in der Energiewirtschaft sind diese beiden Sektoren eng miteinander verflochten, wobei die Bedeutung der Daten- und Informationssicherheit im Energiesektor kontinuierlich zugenommen hat und weiterhin zunimmt. Die Wichtigkeit liegt aber nicht nur in ihrem Vorhandensein, sondern auch in der Korrektheit der Inhalte. Da auf Basis dieser Informationen systemrelevante Entscheidungen getroffen werden, müssen die grundlegenden Informationen und die Interpretation sowie Nutzung und Verarbeitung dieser Daten sorgfältig und kritisch analysiert werden, um deren Richtigkeit sicherzustellen.*

Ausfall kritischer Infrastrukturen

Für einen Ausfall der Stromversorgung können verschiedene Faktoren eine Rolle spielen. Zum Beispiel können physische Ereignisse Schäden an Anlagen des Stromversorgungssystems anrichten, wie an Kraftwerken, Umspannwerken oder Stromleitungen. Ursache dafür können u.a. Bauarbeiten oder schwere Unwetter sein. Weiterhin können aber auch Überlastungen von Betriebsmitteln zu deren Ausfall führen und einen flächendeckenden Stromausfall nach sich ziehen. Ferner können physische Beschädigungen durch technisches Versagen entstehen, ausgelöst durch Alterung, Verschleiß oder Konstruktionsfehler sowie aufgrund mangelhafter Wartung. Im Gegensatz zu Störungen durch Extremwetterereignissen oder Bauarbeiten können diese Situationen mit Vorkehrungsmaßnahmen aber reduziert oder vermieden werden. Darüber hinaus geht zunehmend eine Gefahr von terroristischen Anschlägen oder Sabotagen aus, die für Stromausfälle verantwortlich sein können.

Eine weitere Fehlerquelle, deren Risiko durch den zunehmenden Einsatz datengetriebener Prozesse verstärkt wird, sind Fehler in den Daten selbst. Im Januar 2019 kam es in Europa zu einem Beinahe-Blackout als die Stromfrequenz auf einen kritischen Wert von 49,8 Hz absank. Verantwortlich für den schnellen Frequenzabfall war, aller Wahrscheinlichkeit nach, ein Datenfehler an einem Netzregler im Gebiet des deutschen Übertagungsnetzbetreibers TenneT. Allein mit primärer Regelleistung konnte die Frequenz nicht stabilisiert werden und drohte weiter zu sinken. Durch die schnelle Reaktion des französischen Übertragungsnetzbetreibers RTE, der durch einen Notlastabwurfbefehl bei allen 22 Stromgroßverbrauchern insgesamt 1500 MW vom Netz nehmen konnte, konnte die Netzfrequenz wieder stabilisiert werden. Zusätzlich hat RWE in Deutschland zwei Pumpspeicherkraftwerke zeitgleich hochgefahren. Hierdurch konnte im Zusammenspiel mit dem Lastabwurf in Frankreich die Netzfrequenz wieder den 50 Hz angenähert werden [12].

> *Zukünftig können durch die Veränderungen der Netzinfrastruktur weitere Risiken hinzukommen, die heute noch nicht genau abgeschätzt werden können. Aufgrund der Komplexität des zukünftigen Stromnetzes ist das Systemverhalten schwerer vorauszusagen, durch Abhängigkeiten zwischen Erzeugung, Marktgeschehen und neuartigen Verbrauchern können neue, komplexe Störereignisse auftreten. Ein hohes Gefahrenpotenzial wird beispielsweise aktuell bei der E-Mobilität und einer hohen Gleichzeitigkeit bei Ladevorgängen erwartet.*

2.2 Kritische Prozesse

Das Wort *kritisch*, im Zusammenhang mit Prozessen, soll auf mögliche starke Gefährdungen im Falle von Ab- oder Unterbrechungen dieser Prozesse hinweisen.

Die Gefährdung bei *kritischen Prozessen* in Stromnetzen besteht in erster Linie in dem Ausfall der an die Stromversorgung angeschlossenen, systemrelevanten Verbraucher. Hierzu zählen insbesondere Einrichtungen der öffentlichen Sicherheit und Ordnung wie z.B. Krankenhäuser, Polizei und Feuerwehr. Aber auch weitere Einrichtungen und Anlagen, die bei einem Stromausfall eine Gefahr für das Leben und Wohlergehen von Menschen darstellen. Allerdings muss man hier Abstufungen machen. Auch Prozesse, bei denen nicht unmittelbar Infrastruktur oder Leben in Gefahr sind, müssen bereits als kritisch angesehen werden. So sind die Prozesse, die einen sicheren und stabilen Netzbetrieb darstellen, in der operativen Planung auch bereits mit hinzuzuzählen. Diese werden auch die ersten Prozesse sein, die auf Basis neuer Datengrundlagen und deren Möglichkeiten immer stärker digitalisiert und automatisiert werden können. Somit können grundsätzlich fast alle Aktivitäten, die das physische Stromnetz betreffen, vom Endkunden bis zum Betrieb, als kritisch angesehen werden, da sie bei unsachgemäßer Anwendung zu Netzstörungen beitragen können. Dennoch unterscheiden sich Prozesse in der Höhe ihrer Kritikalität.

Indikatoren, die zur Bestimmung und Einordnung kritischer Prozesse herangezogen werden können, wurden innerhalb dieses Gutachtens analysiert und mit Vertretern einzelner Stromverteilnetzbetreiber gespiegelt[1]. Hierbei sind Prozesse, die in den direkten Systembetrieb eingreifen und essenziell für die Erbringung einer sicheren und stabilen Stromversorgung sind, als kritischer einzustufen als Prozesse, die bei einzelnen Kunden durchgeführt werden, z.B. die Installation von Messeinrichtungen oder der Anschluss von Wallboxen, die maximal Auswirkungen auf diesen einen Kunden haben. Als Indikatoren für die Bewertung der Kritikalität ergeben sich hieraus:

- **Echtzeitnähe und unmittelbare Auswirkungen** für den aktuellen operativen Betrieb. Hier sind im Allgemeinen operative Prozesse kritischer als planerische Prozesse einzustufen. So ist der Prozess der Zielnetzplanung z.B. weniger kritisch als der Prozess der Erstellung und Verarbeitung von Einspeiseprognosen. Bei beiden hat man allerdings noch Zeit für den Fall eines Prozessausfalls für Ersatz bzw. Wiederherstellung zu sorgen. Der Prozess der aktuellen Messwertverarbeitung und evtl. anschließender Zustandsbestimmung ist sehr viel systemrelevanter, da dieser in Echtzeit stattfindet und unmittelbare Konsequenzen auf mögliche Handlungen der Netzoperierenden hat.
- Prinzipiell muss bei allen Prozessen geprüft werden, ob im Fehlerfall beispielsweise die **IKT- und Datensicherheit** gefährdet ist oder Sicherheitslücken für Cyber-Angriffe entstehen. Dies ist z.B. wichtig, wenn in einem Prozess Daten (Messwerte, Netzstrukturen, Betriebsmittel etc.) nach Außen kommuniziert werden oder man von außen auf Daten dieses Prozesses zugreifen kann. Hier ließe sich der aktuelle Redispatch 2.0 Prozess anführen, bei dem z.B. Informationen über Wirksamkeiten von Erzeugungsanlagen auf bestimmte Punkte im Netz (Netzverknüpfungspunkte) an angebundene überlagerte Netzbetreiber kommuniziert werden. Werden diese Daten abgegriffen, lassen sich anhand derer relevante Anlagen für den Redispatch identifizieren und ggf. manipulieren.

[1] Dieses fand im Rahmen von zwei Workshops mit mittleren und großen Verteilnetzbetreibern statt.

- Zusätzlich kann die **Verletzung von Grenzwerten** zur Beurteilung herangezogen werden. Wird z.B. das n-1 Kriterium verletzt, hat dies erst mal noch keine direkte physische Auswirkung auf den Netzbetrieb. Können allerdings bei Fehlern im Prozess oder Ausfall dessen sofortige Betriebsmittelüberlastungen oder andere Grenzwertverletzungen auftreten, befindet sich das Stromnetz in einer kritischen Situation und der Prozess muss als sehr kritisch eingestuft werden. Als Beispiel lässt sich hier der Prozess der Anlagensollwertvorgaben anführen. Wird das Netz mithilfe von Sollwertvorgaben in einen neuen Arbeitspunkt gefahren, müssen diese mithilfe von Netzsicherheitsrechnungen im Vorfeld überprüft und validiert werden. Fehler oder fehlerhafte Datengrundlagen in diesem Prozess können über die Verletzung des n-1-Kriteriums und von Grenzwerten bis hin zu Schäden an Betriebsmitteln und Ausfällen führen.
- **Unterbrechungen oder Ausfall des Prozesses:** Für die Bewertung des Ausfallschadens kann sowohl ein wirtschaftlicher Schaden als auch eine Versorgungsunterbrechung in Bezug auf die Anzahl der betroffenen Kunden oder die Dauer des Ausfalls herangezogen werden. Hier kann man z.B. den Prozess der Fehlerlokalisierung (speziell in MS und NS) anführen und anschließende Isolierung des Fehlers und Wiederversorgung des restlichen Netzgebietes. Ist dieser Prozess fehlerhaft oder fällt aus, verzögert sich z.B. die Lokalisierung eines Kurzschlusses und kann somit zu höherem Schaden am Betriebsmittel und zu längeren Ausfallzeiten führen, was den ASIDI erhöht.

In Tabelle 1 findet sich die Übersicht und Bewertung einer Auswahl an Indikatoren und möglichen Signalfragen (ohne Anspruch auf Vollständigkeit), die als relevant eingeordnet wurden und als Hilfestellung zur Einordnung einzelner Prozesse herangezogen werden können.

Wann ist ein Prozess im Stromnetz kritisch?	*Bewertung*
Indikator: Bewertung der **Echtzeitnähe und unmittelbaren Auswirkungen** des Prozesses. • Ist es ein planerischer oder operativer Prozess? • Beeinflusst der Prozess den direkten Systembetrieb?	Je mehr der Prozess an der operativen Planung oder am operativen Betrieb dran ist, desto kritischer ist dieser einzuschätzen. Beeinflusst dieser Prozess auch noch direkt den operativen Betrieb, dann steigt dieser noch in seiner Kritikalität.
Indikator: Bewertung der **Daten- und Informationssicherheit.** • Sind kritische Daten oder Informationen gefährdet? • Sind personenbezogene Informationen gefährdet? • Können Sicherheitslücken entstehen, die Raum für Cyber-Angriffe bieten?	Bewertung kann über ISMS (Dienstleister -) Selbstauskünfte und Evaluation von Technisch Organisatorischen Maßnahmen (TOMs) erfolgen.
Indikator: Bewertung von **Grenzwertverletzungen** bei Fehlern oder Ausfall des Prozesses. • Kann das n-1 Kriterium verletzt werden?	Unterscheidung nach Art der Grenzwertverletzung und ob mögliche betroffene Betriebsmittel temporäre oder dauerhafte

• Können Betriebsmittelüberlastungen auftreten (Strom- und Spannungsgrenzen)? • Können weitere Grenzwerte verletzt werden (z.B. Lastwinkel/Schutzauslösung)?	Überlastungen aushalten. Je mehr Betriebsmittel betroffen sind und zerstört werden können, desto kritischer ist der Prozess einzustufen.
Indikator: Bewertung des Schadenpotentials/ Ausfallschadens bei **Unterbrechungen oder Ausfall des Prozesses**. • Wie groß ist ein potenzieller finanzieller Schaden? • Kann es zu Versorgungsunterbrechungen kommen (Leistung, Anzahl der betroffenen Kunden, Dauer → Ausfallminuten)?	Je höher der mögliche Schaden ist, umso kritischer ist der Prozess, sowohl in finanzieller Hinsicht als auch bei Versorgungsunterbrechungen.

Tabelle 1: Definierte Indikatoren zur Beurteilung der Kritikalität von Prozessen im Stromnetz.

Anhand dieser Indikatoren können einzelne Prozesse analysiert und bzgl. ihrer Kritikalität und Schadenpotenzials eingeordnet und evaluiert werden. In Abbildung 2 wurde den einzelnen Indikatoren ihre Relevanz bzgl. pot. Schädlichkeit innerhalb der Bereiche des Netzbetriebs, der IKT-Sicherheit, der Netzbetriebsführung und operativen Planung, Instandhaltung sowie dem Endkundenbereich zugeordnet. Die einzelnen Bereiche werden im Folgenden kurz beschrieben.

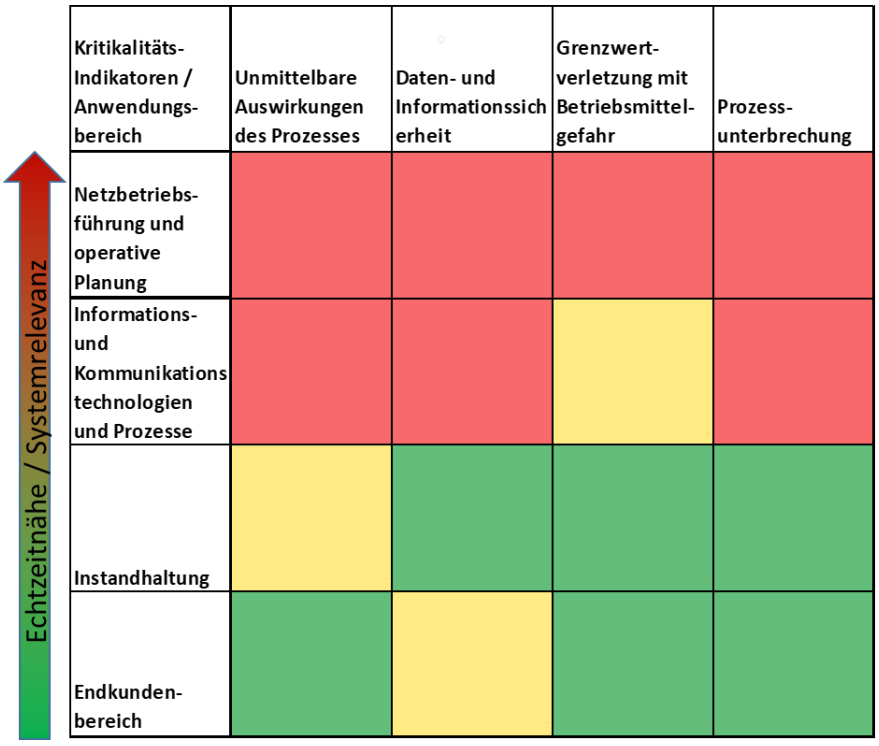


Abbildung 2: Einschätzung der Kritikalitäts-Indikatoren in verschiedenen Bereichen des Netzbetriebs. Grün steht für unkritisch mit geringem Schadenpotenzial, rot steht für sehr kritisch mit hohem Schadenpotenzial.

2.2.1 Netzbetriebsführung und operative Netzplanung

Prozesse der operativen Netzbetriebsführung sind als besonders kritisch einzustufen, da diese einen direkten Einfluss auf den Systembetrieb haben. Prozesse in der Netzbetriebsführung müssen zuverlässig die Frequenz und Spannung innerhalb der zulässigen Grenzwerte halten sowie thermische Überlastungen von Betriebsmitteln vermeiden. Ein Fehler in der Systemführung kann kaskadenartig fortschreiten und zu großflächigen Stromausfällen führen. Auch die operative Netzplanung trägt dazu bei Grenzwertverletzungen, wie z.B. Leitungsüberlastungen, im Vorfeld zu verhindern, indem eine gezielte Kraftwerkseinsatzplanung, in Abstimmung mit Einspeise- und Verbrauchsprognosen umgesetzt wird. Auch der Netzwiederaufbau und die schnelle Netzwiederversorgung nach Störungen lassen sich in diesen Bereich einordnen.

> *Der kritischste Bereich bzw. die kritischsten Prozesse gehören der Netzbetriebsführung und operativen Netzplanung an, da diese Prozesse eine direkte Auswirkung auf den Systembetrieb haben und mögliche Fehler sich unmittelbar auswirken und es wenig bis gar keine Zeit zur Korrektur gibt. Daher sollten insbesondere neue innovative Prozesse der operativen Betriebsführung besonders kritisch auf mögliche Gefahren in den Datengrundlagen aber auch in der Umsetzung hin geprüft werden.*

2.2.2 Informations- und Kommunikationstechnologie (IKT)

Einen besonderen Stellenwert im Rahmen der Digitalisierung und datengetriebener Prozesse nimmt die Informations- und Kommunikationstechnologie ein, da die große Teilnehmerzahl dezentraler Netznutzer eine rasant steigende Menge an Daten produziert [12]. Als eigener Sektor durchdringen IKT-Prozesse alle Bereiche der Energieversorgung, weshalb der IKT-Sicherheit eine übergeordnete Rolle zukommt.

Mit der massenhaften Erfassung von Daten und deren weiteren Verwendung in Datenanalysen und intelligenten Anwendungen steigen auch die datenbasierten Risiken. Hierzu zählen z.B. Datenmanipulationen, durch die kritische Situationen entstehen können, sowie die Datenübertragung selbst als kritischer Prozess. Datenbasierte Risiken werden in Kapitel 3.3 beschrieben. Die steigende Menge an Daten macht das Stromnetz zudem anfälliger für Hacker-Angriffe. Diese Cyber-Angriffe stellen ein ernstzunehmendes Risiko für einen flächendeckenden Stromausfall dar [22] [12].

Dass ein Hackerangriff auf das Stromnetz möglich und nicht unwahrscheinlich ist, zeigen die Angriffe auf das ukrainische Stromnetz. Gerade in Kriegssituationen kann das Stromnetz ein Ziel für Cyberattacken werden, wie bei dem kürzlich versuchten Angriff im April 2022, der durch einen anonymen Hinweis aber vereitelt werden konnte. Ziel des Angriffs sollen hier verschiedene Umspannwerke gewesen sein [23]. Die vermutlich gleiche Gruppe hatte bereits in den Jahren 2015 und 2016 bei einem Cyberangriff auf die Computer- und SCADA-Systeme die Stromversorgung in der Ukraine für mehrere Stunden unterbrochen. Auch hierbei wurden 30 Umspannwerke durch die Hacker abgeschaltet, wodurch mehrere hunderttausend Haushalte stundenlang ohne Strom auskommen mussten [25]. Der Angriff damals hat gezeigt, dass durch einen groß angelegten, koordinierten Hacker-Angriff der Strom flächendeckend ausgeschaltet werden kann. Ein Blackout kann eine signifikante Bedrohung sein [26].

Um Cyber-Angriffen und Manipulationen vorzubeugen, gelten in Deutschland gesetzliche Vorgaben für Stromnetzbetreiber, die im IT-Sicherheitskatalog der Bundesnetzagentur zusammengefasst sind. Netzbetreiber sind hierdurch verpflichtet ein Informations-Sicherheits-Maßnahmen-System (ISMS) zu implementieren, das den dort beschriebenen Anforderungen genügt (vgl. Kapitel 4.1) [28].

> *Die Sicherheit der Informations- und Kommunikationstechnologien ist der zentrale Punkt, wenn es zukünftig um datengetriebene kritische Prozesse geht. Die Integrität und Sicherheit der Daten entlang der gesamten Wertschöpfungskette muss zu jederzeit gewährleistet sein, um eine stabile und zuverlässige Versorgung mit Energie garantieren zu können.*

2.2.3 Instandhaltung

Für eine funktionierende und zuverlässige Stromversorgung ist die Instandhaltung der verschiedenen Netzelemente (z.B. IKT-Anlagen) und Betriebsmittel (Leitungen, Transformatoren etc.) notwendig. Dennoch sind Instandhaltungsmaßnahmen als weniger kritisch einzustufen, da diese im Regelfall gut planbar sind und Störungen meist kleinere lokale Gebiete betreffen. Zu typischen Wartungs- und Instandhaltungsmaßnahmen gehören u.a. die Inspektion der Betriebsmittel zur Beurteilung des Ist-Zustands sowie die Wartung als Maßnahme zur Erhaltung des Soll-Zustands (z.B. durch Ersetzen und Erneuern von Komponenten) zur Sicherstellung der Funktionsfähigkeit. Der Bereich der vorausschauenden Wartung zielt darauf ab, alternde und potenziell defekte Komponenten zu erkennen und zu ersetzen, bevor sie ausfallen. Weiterhin zählen die Instandsetzung zur Wiederherstellung des Soll-Zustands nach einem Defekt oder Ausfall und die Verbesserung als technische und administrative Maßnahme zur Steigerung der Funktionssicherheit zu Instandhaltungsmaßnahmen.

> *Instandhaltungsprozesse können zwar durchaus zu einer kritischen Situation führen, sind aber nicht in gleichem Maße kritisch wie die Systemführung, da diese Prozesse meist planbar sind und somit zu Zeiten durchgeführt werden können, in denen systemweite Einflüsse minimiert sind.*

2.2.4 Endkundenbereich

Den unkritischsten Bereich bildet der Endkundenbereich. Zu diesem Bereich gehören beispielsweise Prozesse, die den Zähler- und Anschlussbetrieb betreffen. Diese beeinflussen zumeist lediglich einen einzelnen Kunden und haben keinen oder nur geringen Einfluss auf weitere Netznutzer, sodass diese Prozesse als nicht kritisch einzustufen sind. Auch ein angepasstes Verbrauchsverhalten gehört in diesen Bereich. Hierbei passen Kunden ihren Strombedarf entsprechend der aktuellen Verfügbarkeit an und erhalten im Gegenzug einen günstigeren Strompreis.

> *Am unkritischsten sind Prozesse aus dem Endkundenbereich, da diese meist nur Einfluss auf einen einzelnen Kunden haben und die Systemstabilität respektive allgemeine Versorgung nicht beeinflussen.*

Abschließend lässt sich sagen, dass fast alle Prozesse in einer kritischen Infrastruktur, bzw. einem kritischen Umfeld als kritisch einzustufen sind. Die Frage, die allerdings im Folgenden erläutert werden soll, ist wie sich die Nutzung von Algorithmen künstlicher Intelligenz (KI) und die dazu notwendigen Daten und Datenflüsse in diese Prozesse einordnen lassen. Festzustellen ist, dass

wenn KI-Anwendungen in Prozessen in kritischen Umgebungen Anwendung finden sollen, diese sich an bestehende Prozesse anlehnen und diese unterstützen sollten und im Endeffekt dafür Sorge tragen, dass Prozessausfälle weniger drastische Auswirkungen haben.

2.3 Datenanalysen und intelligente Anwendungen

Digitalisierte Netze und neue Messsysteme, die, in Verbindung mit neuen Technologien, eine massenhafte Erfassung von Daten ermöglichen, bieten ein vielfältiges Potential für Datenanalysen und intelligente Anwendungen, z.B. um Prozesse zu optimieren. Bei dem Einsatz solcher Anwendungen muss mit Blick auf kritische Prozesse genau analysiert werden, welche Auswirkungen die Anwendung auf den jeweiligen Prozess haben kann. So kann beispielsweise der Betrieb von Freileitungen, mithilfe neuer Verfahren zur Datenerfassung und –übertragung, effizienter gestaltet werden, in dem man Informationen über die aktuellen und zukünftigen Wetterverhältnisse berücksichtigt. Typischerweise sind für Freileitungen normierte Dauerstrombelastungen definiert. Da die Kapazität der Freileitungen jedoch stark von den Witterungsbedingungen abhängt, können sich niedrige Temperaturen oder hohe Windgeschwindigkeiten teilweise positiv auf die Dauerstrombelastbarkeit auswirken. Werden aktuelle Wetterdaten im Betrieb berücksichtigt, können zeitweise höhere Ströme übertragen werden, ohne Grenzwerte, wie die maximale Betriebstemperatur oder den maximalen Durchhang, zu überschreiten [20]. Effektiv lässt sich die Kapazität erhöhen.

Für einen stabilen und sicheren Netzbetrieb müssen zahlreiche Einflussfaktoren (häufig in Echtzeit) berücksichtigt werden, wofür in kurzer Zeit eine große Menge an Daten ausgewertet werden muss, um den Netzbetrieb nicht zu gefährden. Zeitgleich zu den stetig wachsenden Datenmengen werden auch kontinuierlich Fortschritte in der Rechen- und Speichertechnik gemacht. So können beispielsweise durch den Einsatz moderner Datenbanksysteme neue Dateninfrastrukturen aufgebaut werden. Um die anfallenden Datenmengen bewältigen zu können, ist der Einsatz innovativer Datenverarbeitungsmethoden notwendig [14]. Hier wurden insbesondere auf dem Gebiet des maschinellen Lernens und der künstlichen Intelligenz enorme Fortschritte in Bereich „Big Data“ gemacht.

> *Daher wird es im Rahmen dieses Gutachtens als nächsten logischen Schritt angesehen, Methoden der künstlichen Intelligenz und des maschinellen Lernens zukünftig vermehrt zur Bewältigung der immer größer werdenden Datenmengen zu benutzen.*

Datenanalyse und Künstliche Intelligenz

Wie in den vorherigen Abschnitten bereits erwähnt, werden im Zuge der Digitalisierung aus immer mehr Quellen immer weitere Daten gewonnen. So liefern z.B. Smart-Meter viertelstundenscharfe Messungen, Wechselrichter senden ihre Zustands- und Messdaten an Server der Hersteller (in der Regel zu Wartungszwecken), Prognosen und Einsatzpläne umspannen zum Teil schon Zeitbereiche bis zu einer Woche und werden teilweise stündlich aktualisiert. Die Menge an Informationen, die aus dem Stromnetz und über das Stromnetz verfügbar ist und ständig neu produziert wird, ist auf ein bisher nicht dagewesenes Maximum angewachsen und steigt stetig weiter an. Diese Datengrundlage bietet, wie hier und unter 1.2.1 bereits erwähnt, neue Chancen aber auch Herausforderungen. Eine grundlegende Herausforderung ist zunächst diese Menge an Daten zu strukturieren, analysieren und archivieren. Um neben den direkten Analysen der Daten weiteren Mehrwert zu

erzeugen, ist es wichtig Korrelationen der verschiedenen Datenquellen und –arten zu identifizieren und zu nutzen. Hier rückt die bereits mehrfach erwähnte künstliche Intelligenz oder auch das maschinelle Lernen in den Fokus.

Der Begriff der Künstlichen Intelligenz (KI) entwickelt sich derzeit fortlaufend weiter. Von der „High Level Expert Group on Artificial Intelligence" der Europäischen Kommission wird KI wie folgt definiert:

> *„Von Menschen entworfene Soft- und Hardwaresysteme, die – ein komplexes Ziel gegeben – in der physischen oder digitalen Dimension agieren. Dies geschieht, indem sie ihre Umgebung mittels Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren und durch Schlussfolgerung die aus diesen Daten abgeleiteten Informationen für die Entscheidung über die besten Maßnahmen zur Erreichung des vorgegebenen Ziels nutzen. Ein solches System kann symbolische Regeln verwenden oder numerische Modelle lernen und kann außerdem sein Verhalten anpassen, indem es analysiert, wie die Umgebung durch seine vorherigen Aktionen beeinflusst wurde."*

Grundsätzlich kann KI in zwei Kategorien unterteilt werden, die sogenannte starke und schwache KI. Das Prinzip der starken KI beschreibt die maschinelle Nachbildung der kognitiven Fähigkeiten des Menschen, die sogar übertroffen werden können. Dieses Konzept ist aktuell aber nicht Stand der Technik und kommt im Stromnetz nicht zum Einsatz. Bei der schwachen KI liegt der Fokus auf Anwendungsproblemen, die basierend auf mathematischen Methoden oder Methoden aus der Informatik gelöst werden [43]. Data Mining, Machine Learning (ML) und Deep Learning sowie künstliche neuronale Netze (KNN) bilden beispielsweise Teilgebiete der künstlichen Intelligenz. Die verschiedenen Arten der künstlichen Intelligenz und deren Unterschiede werden in der dena-Analyse „Künstliche Intelligenz für die integrierte Energiewende" ausführlich erklärt [1]. Methoden der künstlichen Intelligenz können helfen die enormen Datenmengen zu bewältigen und z.B. durch Korrelation verschiedener Datenquellen oder Mustererkennung im Datensatz, vorhandenes Potenzial zur Verbesserung von Prozessen oder Entwicklung neuer Prozesse und Anwendungen optimal zu nutzen. Im Vergleich zu herkömmlichen Methoden sind KI-Methoden diesen z.B. vor allem in Schnelligkeit oft überlegen. Außerdem besitzen sie die Fähigkeit Strukturen oder Muster in großen Datenmengen zu erkennen und sogar unstrukturierte Daten in eine aussagekräftige Form zu bringen [43]. So lassen sich bereits heutzutage vorrausschauende Wartungsarbeiten mithilfe von KI optimal planen, sodass diese nicht zu spät stattfinden und es schon zu Schäden am Betriebsmittel gekommen ist, aber auch nicht zu früh und so unnötig Ersatzteile gewechselt werden und Zeit investiert wird.

„PricewaterhouseCoopers (PwC) schätzt das zusätzliche Wertschöpfungspotenzial, welches durch eine konsequente Nutzung von künstlicher Intelligenz (KI) im deutschen Energiesektor bis zum Jahr 2030 erreicht werden soll, auf ca. 30 Mrd. Euro, was einem Anteil von 6,8 % an der gesamten zusätzlichen Wertschöpfung entspricht. [12]"

Im November 2018 wurde von der Bundesregierung im Rahmen der Umsetzungsstrategie Digitalisierung eine KI-Strategie verabschiedet, die u.a. Ziele beinhaltet, die die künftige Wettbewerbsfähigkeit Deutschlands sichern sollen. Hierbei soll die Entwicklung und der Einsatz von künstlicher Intelligenz verantwortungsvoll und gemeinwohlorientiert vorangebracht werden (siehe Kapitel 4.2). Im Stromnetz sind derzeit bereits KI-Anwendungen erfolgreich im Einsatz, so

z.B. bei einem Verteilnetzbetreiber, der ein Frühwarnsystem für Störungen in Umspannwerken entwickelt hat, das auf KI basiert (siehe 5.2.3).

Wenn hier und im Folgenden von KI-Anwendungen gesprochen wird, sind Anwendungen gemeint, die Methoden der künstlichen Intelligenz, wie z.B. künstliche neuronale Netze, nutzen.

> *KI-Anwendungen bieten für die Energiebranche, und hier betrachten wir speziell den Netzbetrieb, neue Möglichkeiten aus der bereits vorhandenen und stetig wachsenden Datenmenge Mehrwerte für den Netzbetrieb zu generieren. Die Strukturierung, Analyse und Korrelation der verschiedenen Daten untereinander hat das Potenzial Betriebsführungen präziser und somit effizienter zu machen (z.B. führen genauere Energie- und Netzzustandsprognosen zu passenderen Entscheidungen für den Netzbetrieb). Diese neue, sich abzeichnende Abhängigkeit von Daten und deren Verwertung führt aber auch zu neuen Risiken. Diese müssen, insbesondere im Umfeld der kritischen Infrastruktur, frühzeitig adressiert und mit entsprechenden Vorsichtsmaßnahmen behandelt werden.*

2.3.1 Risiken bei der Anwendung von Datenanalysen und KI

Neben den Vorteilen und neuen Möglichkeiten die KI-Anwendungen mit sich bringen, bürgen sie aber auch neue Risiken. In dem Gesetzesvorschlag zur „Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz)“ werden einige KI-Systeme als hochriskant eingestuft oder sogar explizit verboten. Als hochriskant eingestuft werden Systeme, die zur Verwaltung und zum Betrieb kritischer Infrastrukturen eingesetzt werden, worunter die Stromversorgung fällt (vgl. Kapitel 2).

Grundlegend unterliegen KI-Systeme hinsichtlich der **Datenabhängigkeit** den gleichen Schwachstellen wie andere traditionelle Methoden. Das bedeutet, dass Sensorfehler, fehlende Daten, Datenmanipulationen durch Hacker und andere datenbezogene Fehler KI-Systeme genauso beeinträchtigen werden, wie dies bei früheren Methoden der Fall war. Da KI-Anwendungen jedoch in der Regel größere Datenmengen und potenziell neue Datenquellen nutzen können, die von einfacheren Methoden nicht verwendet werden, können KI-Methoden unter Umständen ein höheres Maß an Anfälligkeit für Datenfehler aufweisen. Daher muss darauf geachtet werden, dass die erhöhte Abhängigkeit von Daten mit einem hohen Maß an Genauigkeit und Zuverlässigkeit einhergeht.

Ein weiteres Risiko liegt in dem **Niveau der Leistung,** die eine KI erreichen kann. Dieses kann so hoch sein, dass das System Entscheidungen vorschlägt, die rational nicht mehr nachvollziehbar und von Menschen auch nicht mehr reproduzierbar sind (*übermenschliches Niveau*). Somit kann, sowohl in Bezug auf die wirtschaftliche Rentabilität als auch auf die Netzsicherheit, die Frage der Abhängigkeit von der Automatisierung durch eine KI eine zentrale Rolle spielen. Dieses Phänomen ist z.B. bereits aus der Luftfahrtindustrie bekannt, wo ein übermäßiges Vertrauen in den Autopiloten zu kritischen Situationen führen kann, wenn Situationen nur noch durch diesen zu bewältigen sind.

Hier lässt sich auch auf eine fehlende **Nachvollziehbarkeit** der Ergebnisse hinweisen. Durch die Art und Weise wie künstliche Intelligenzen lernen, bzw. trainiert werden, lassen sich die zugrunde-

liegenden Strukturen in den Daten, die später die Grundlage für die Ergebnisse und Entscheidungen bilden, als Mensch nicht erkennen und somit auch die Ergebnisse nicht nachvollziehen. Solche Anwendungen werden auch als *Black-Box KI* [44] bezeichnet und können ein Risiko darstellen, da die Ergebnisse nicht unabhängig von der Anwendung geprüft und validiert werden können.

Selbst die am besten getestete KI kann fehleranfällig sein, beispielsweise, wenn sie auf eine Situation stößt, die nicht in ihren Trainingsdaten enthalten war, oder aufgrund eines Fehlers oder einer Ungenauigkeit in einer Eingabedatenquelle. **Übermäßiges Vertrauen (Automation Bias)** in eine künstliche Intelligenz tritt auf, wenn ein Bediener zu viel Vertrauen in das Urteil eines automatisierten Systems setzt, selbst angesichts widersprüchlicher Signale von parallelen Systemen im Kontrollraum. Eine weitere Form von übersteigertem Vertrauen in die Automatisierung (automation complacency) ist, wenn sich der Bediener darauf verlässt, dass die Automatisierung alle Probleme meldet und in der Folge aufhört aktiv das Geschehen zu verfolgen. Hierdurch können Probleme übersehen werden, die zuvor bei einer aktiven Überwachung nicht übersehen worden wären. Experten für Verhaltenspsychologie haben unsere angeborene Tendenz, in Technologien zu vertrauen, eingehend untersucht mit dem Ergebnis, dass dieses Verhalten bei einem voll automatisierten Netzbetrieb ebenfalls auftreten wird [17][18].

> *Aktuell gibt es, wenn überhaupt, nur wenige KI-Anwendungen in der Praxis, die automatisierte Aktionen im Netz durchführen, die zu kritischen Netzsituationen führen können. Die meisten dieser potenziellen Anwendungen würden einen "Human-in-the-Loop"-Betrieb erfordern, bei dem die Entscheidungen selbst bei den für das System verantwortlichen Mitarbeitenden bleiben. Optimierungsverfahren können Handlungsempfehlungen geben und bei Entscheidungen unterstützen, sie übernehmen in der Regel aber nicht automatisiert den Netzbetrieb. Entscheidungen selbst liegen weiterhin bei dem systemverantwortlichen Personal.*

Für einen möglichst sicheren und risikominimierten Einsatz neuartiger Anwendungen sollten bestimmte Anforderungen eingehalten werden (siehe hierzu auch Kapitel 5). So müssen in der Anfangsphase die Ergebnisse neuer Anwendungen kritisch überprüft werden, sowohl um die Richtigkeit der Anwendung zu überprüfen als auch um Vertrauen in die Funktionalität aufzubauen und Akzeptanz im Unternehmen zu gewinnen. Hierfür kann z.B. ein Vergleich der Ergebnisse der neuen Anwendung mit den Ergebnissen einer klassischen Methode erfolgen, sofern diese vorhanden ist. Wenn möglich kann auch ein Parallelbetrieb erfolgen, bis auf Erfahrungen vertraut werden kann. Um das Risiko kritischer Situationen, die durch diese Anwendungen ausgelöst werden können, zu minimieren, gelten für diese Systeme zusätzlich bestimmte Anforderungen. Als Beispiele sind hier ein Back-Up Plan für den Notfall zu nennen sowie eine Eingriffsmöglichkeit, die sogenannte Stop-Button-Vorschrift, um KI-Systeme stoppen zu können (siehe hierzu auch Kapitel 4.2 „Gesetz über künstliche Intelligenz“).

> *Das ganze Ausmaß möglicher Fehlerquellen, die die Digitalisierung und KI mit sich bringen, ist bisher nicht eindeutig abzuschätzen. Eines der Hauptrisiken wird aber die Abhängigkeit von den jeweiligen Datengrundlagen sein und die mögliche sich aufbauende Abhängigkeit von den Entscheidungen der KI-Systeme. Hinzu kommt die bereits bestehende gegenseitige Abhängigkeit zwischen der Stromversorgung und der IKT. Bricht der Datenstrom ab, droh die Stromversorgung einzubrechen. Bricht aber die Stromversorgung zusammen, droht auch den meisten IKT-Systemen ein Abbruch ihrer Aufgaben, was dann einen möglichen Wiederaufbau der*

Stromversorgung erschwert. Hierfür benötigt es klar definierte Strategien, um sowohl die Risiken zur Entstehung von Versorgungsausfällen zu minimieren als auch im Fehlerfall möglichst schnell das Netz zu stabilisieren.

Im Umgang mit unbekannten Situationen hat sich das Konzept der Resilienz als geeignet erwiesen. „Resilienz bedeutet, die Auswirkungen eines Störereignisses abzufangen – im schlimmsten Fall je nach Konstellation auch mit kurzzeitig abnehmender Versorgungsqualität, ohne dass das System kollabiert, um anschließend zügig wieder in den normalen Betriebszustand zurückzukehren. [19]" Die Arbeitsgruppe „Resilienz digitalisierter Energiesysteme" des Akademienprojekts „Energiesysteme der Zukunft" hat dafür eine Resilienzstrategie entwickelt, die Handlungsfelder mit 15 Handlungsoptionen beinhaltet [19]. Dieses muss zukünftig insbesondere bei der Verwendung von KI-Anwendungen berücksichtigt werden um die Risiken die diese mitbringen zu minimieren.

2.3.2 Anwendungsfelder für intelligente Anwendungen im Stromnetz

Bereits jetzt sind im Stromnetz zahlreiche Anwendungsfelder bekannt, in denen Datenanalysen und KI-Anwendungen vielversprechende Lösungsansätze bieten. So ist es z.B. aufgrund der steigenden Komplexität der Netzteilnehmer immer wichtiger den Zustand des Netzes zu kennen, um z.B. drohende Grenzwertverletzungen zu identifizieren und diese anschließend zu vermeiden. Auch im Falle eines Stromausfalls ist es essentiell den Netzzustand davor und danach für eine Fehleridentifikation und schnelle Wiederversorgung zu kennen. Die Mittel- und Niederspannung sind aber, im Gegensatz zu höheren Spannungsebenen, kaum ausgemessen, was den Einsatz klassischer Verfahren zur Netzzustandsschätzung nur mit zusätzlichen sogenannten Pseudomesswerten ermöglicht. Meist sind nur vereinzelt Messstellen an Umspannwerken oder Ortsnetzstationen installiert. Eine ausreichende Datengrundlage für herkömmliche Verfahren würde nur erreicht werden, wenn die gesamten Mittel- und Niederspannungsnetze mit entsprechender Messtechnik und Sensorik ausgestattet werden würden, was mit enormen Kosten verbunden wäre. Eine Netzzustandsschätzung mithilfe neuronaler Netze kommt hingegen mit weniger Messstellen aus und kann den Zustand des gesamten Netzes schätzen – eine Alternative, die sich zumindest für den Übergang in ein ausgemessenes System lohnen kann bzw. ein neues Kosten-Nutzen Optimum darstellt.

Ein weiterer Bereich, in dem KI-Methoden bereits heute verbreitet sind, sind Wetter- bzw. Energie-Prognosen. Hier werden neben den Informationen der Wetterdienste zusätzlich historische und aktuelle Messwerte von zu prognostizierenden Erzeugungsanlagen verwendet. Diese können mithilfe von KI-Anwendungen miteinander korreliert werden und helfen Berechnungen zur lokalen Netzauslastung zu verbessern, wodurch kritische Zustände frühzeitig erkannt werden können (Einspeisung + Entnahme) [1].

KI-Anwendungen werden aktuell und zukünftig vermehrt in den Bereichen eingesetzt werden, in denen durch Verbindung verschiedener Datenquellen ein (neuer oder zusätzlicher) Mehrwert geschaffen werden kann. Hier liegen auch die Stärke und der Vorteil in der Verwendung von KI-Algorithmen. Wo herkömmliche mathematische Ansätze aufgrund mangelnder oder zu ungenauer Messungen an ihre Grenzen stoßen, können KI-Anwendungen z.T. erhebliche Schritte weitergehen und so aktuelle Herausforderungen des Netzbetriebs bei seiner Transformation zu einem digitalisierten und automatisierten Betrieb unterstützen.

Im Folgenden wird abschließend eine Übersicht über mögliche Anwendungen im Stromnetz gegeben, die KI-Methoden nutzen und deren Einsatz einen Mehrwert gegenüber dem status quo bietet. Der Mehrwert wurde in Bezug auf eine erweiterte oder neue Funktionalität, Prozessoptimierung oder auch in finanzieller Hinsicht evaluiert. Diese Anwendungen können auch teilweise dazu beitragen (kritische oder ungewünschte) Situationen frühzeitig zu erkennen und zu beherrschen und so deren Entstehung zu vermeiden.

Für eine bessere Einordnung mit Bezug auf die in Kapitel 2 beschriebenen kritischen Prozesse sind die einzelnen Anwendungen, sogenannte Use Cases, in die in den Kapiteln 2.2.1 bis 2.2.4 beschriebenen Bereiche eingeordnet.

Es ist noch zu erwähnen, dass es sich bei der Liste lediglich um eine Auswahl an Anwendungen handelt, die keinen Anspruch auf Vollständigkeit erhebt. Eine vollständige Übersicht würde über den Rahmen dieses Gutachtens hinausgehen, besonders da stetig an neuen Anwendungen geforscht wird. In der Beschreibung werden eigene Erfahrungen aus der Arbeit in Projekten und mit VNBs wiedergegeben.

Übersicht ausgewählter Use Cases datengetriebener Prozesse und Analysen für den Netzbetrieb innerhalb der Bereiche kritischer Prozesse

Bereich	Beschreibung	Mehrwert
Netzbetriebsführung & op. Netzplanung	**Netzzustandsbestimmung in MS- und NS-Netzen**	
	MS- und NS-Netze verfügen über nur wenige Messeinrichtungen, sodass die Verfahren der Zustandsschätzung für HS- oder HöS-Netze nicht angewendet werden können. Aufgrund der zunehmenden Komplexität in den Verteilnetzen ist es jedoch wichtig den Netzzustand auch in diesen Netzebenen zu kennen. Künstliche neuronale Netze (KNN) sind in der Lage die elektrischen Variablen auf Basis von historischen Last- und Erzeugungszeitreihen mit geringer Abweichung zu schätzen (wenn die Datengrundlage ausreichend ist). *Sonderfall*: Netzzustandsbestimmung mit dynamischer Topologie	Sichtbarkeit: Erkennung von Grenzwertverletzungen in der MS- und NS-Ebene (Spannungsbandverletzungen, Betriebsmittelüberlastungen), Grundlage zur Ermittlung von Flexibilitäten *Mit dyn. Topologie*: Zusätzlich zu obigen Punkten noch relevant für Schalthandlungen sowie bei der Netzwiederversorgung nach einem Kurzschluss.
	Netzoptimierung durch KI-OPF	
	Die Rechenzeit traditioneller OPF-Methoden nimmt mit hochkomplexen Systemen dramatisch zu. Künstliche Neuronale Netze können lernen, mit Hilfe von historischen und simulierten Daten das OPF-Problem für ein gegebenes Netz zu lösen. Der	Engpässe und Überlastungen vermeiden/ lösen, Systemkostenreduzierung , Bestimmung und Steuerung von Flexibilität,

Netzbetriebsführung & op. Netzplanung	Trainingsprozess findet im Vorfeld statt, sodass die Rechenzeit im Einsatz nur noch Sekunden betragen kann.	Beschleunigung um Größenordnungen gegenüber klassischen OPF Methoden
	Netzbetriebsführung mit Agenten	
	Ein aufstrebender Ansatz aus dem KI-Bereich des Reinforcement Learning. KI-"Agenten" werden mit Belohnungen und Strafen trainiert, um Maßnahmen und Aktionen für den Netzwerkbetrieb vorzuschlagen (Sollwertvorgaben, Schaltsignale etc.), um kritische Situationen zu lösen. Sie können somit das automatisierte Äquivalent zum Netzführer darstellen. Sie sind in der Lage auch mehrstufige Entscheidungen zu treffen und deren Umsetzung vorzuschlagen.	Versorgungssicherheit, Risikoreduzierung, Systemkostenreduzierung
	Netzäquivalente	
	Im modernen elektrischen Netz sind viele Netz-systeme miteinander gekoppelt. Zur Analyse eines Netzbereiches werden die anderen gekoppelten Netzbereiche in der Regel durch ein reduziertes bzw. ein äquivalentes Modell dargestellt, dass das Verhalten des Originalsystems approximieren kann. Mit KNN können die Betriebsfälle des originalen Netzes bei erheblich reduzierter Rechenzeit gegenüber herkömmlichen Verfahren und guter Genauigkeit adaptiv approximiert werden [46].	Verbessertes Wirk- und Blindleistung-smanagement, Untersuchung der Ausgleichsvorgänge beim Zu- und Abschalten von Netzteilen oder im Fehlerfall, Anonymisierte Weitergabe von Netzmodellen
	Detektion von Inselnetzen	
	In Folge von Netzfehlern können sich einzelne Abschnitte im Netz abtrennen. Wenn darüber hinaus ein lokales Leistungsgleichgewicht vorliegt, kann es zur Bildung von ungewollten Inselnetzen kommen. Zur Vorbeugung von Personen- und Anlagenschäden müssen die ungewollten Inselnetze lokal detektiert und anschließend gezielt destabilisiert werden.	Erkennung von abgetrennten Netzbereichen und Vermeidung von Schäden an Personen oder Anlagen
	Witterungsabhängiger Freileitungsbetrieb (WAFB)	
	Um höhere Übertragungsreserven im Stromnetz zu realisieren, gilt Netzoptimierung vor Verstärkung	Erhöhung der Übertragungspotentiale/

Netzbetriebsführung & op. Netzplanung	vor Ausbau. Bei einem witterungsabhängigen Freileitungsbetrieb lassen sich insbesondere in den windreichen und kalten Jahreszeiten anhand von Datenanalysen höhere Übertragungskapazitäten realisieren, da die thermische Strombelastbarkeit der Leiter steigt.	Reserven, Entlastungen bei Überlastungen anderer Leiter
	Nutzung von Wasserstoff	
	Wasserstoff Elektrolyse entwickelt sich als eine Möglichkeit, die Überproduktion erneuerbarer Energien wirtschaftlich zu bewältigen und Energiesektoren zu koppeln. Der Betrieb der Elektrolyseure erfolgt dabei netzunterstützend. KI wird eingesetzt, um deren Leistung im Netz zu optimieren und optimale Regeltechniken zu entwickeln.	Netzstabilität, zusätzliche Flexibilitäten durch Sektorenkopplung, Vermeidung von Abregelungen
	Lademanagement	
	Die Menge gleichzeitiger Ladevorgänge in Kombination mit der aktuellen Netzsituation kann zu kritischen Netzsituationen führen. KI-Methoden können Netzbetreiber unterstützen Ladevorgänge optimal zu steuern und dynamisch an die Netzkapazität anzupassen sowie bestehende Netze höher auszulasten.	Beherrschung des Systemverhaltens, Vermeidung von Leitungsüberlastungen
	Gleichzeitigkeitsberechnung	
	In der Netzplanung werden die Netze üblicherweise mit Bezug auf den schlimmsten, noch realistischerweise anzunehmenden Lastfall ausgelegt. Um die hierfür notwendigen Gleichzeitigkeiten zwischen Haushalten und neuen Verbrauchern wie E-Kfz und Wärmepumpen korrekt abzubilden, bedarf es aufwendiger Berechnungen. KI-Methoden erlauben die Gleichzeitigkeit mit geringem Fehler zu approximieren und sind dabei wesentlich performanter.	Präzise Berechnung der Netzauslastung. Vermeidung von Überdimensionierung von Betriebsmittel.
	Positionierung öffentlicher Ladestationen/ Standortmanagement (privat & öffentlich)	
	Der Gesamtbedarf an öffentlichen Ladestationen ist ein wichtiger Parameter für den Ausbau der	Verbesserung der Netzinfrastruktur, Erhöhung der Kundenzufriedenheit

Netzbetriebsführung & op. Netzplanung	Ladeinfrastruktur. KI-Methoden können helfen den Bedarf zu bestimmen und an welchen Punkten die Errichtung von Ladestationen sinnvoll ist.	
	Probabilistische Netzzustandsprognosen	
	Ein zuverlässiger Netzbetrieb ist abhängig von genauen Wetter- und Energieprognosen. Auf deren Basis kann der Netzzustand geschätzt werden. Bei fehlerhaften Prognosen können fehlerhafte Regelungen und damit Engpässe oder Überbelastungen entstehen. KI-Methoden bieten intelligente Analysen und Bewertungen zu Eintrittswahrscheinlichkeiten und sprechen Empfehlungen aus.	Vermeidung von kritischen Situationen, Stabilisierung der Energiemärkte, Effizientere Energienutzung, geringere Kosten, steigende Margen
	Einspeiseprognosen	
	Genaue Prognosen für PV-Anlagen und Windparks sind wichtig für den sicheren Betrieb von Stromnetzen. KI-Methoden verbessern die Genauigkeit von Einspeiseprognosen z.B. durch hoch aufgelöste Satellitendaten, wobei Verfahren aus der Bilderkennung und Videoverarbeitung zum Einsatz kommen.	Verbesserung der Prognosegüte
	Lastzeitreihen	
	Lastzeitreihen sind die Grundlage vieler Anwendungen, jedoch aufgrund der Datenverfügbarkeit und unter Beachtung des Datenschutzes ein kritisches Thema. Mit Hilfe von KI-Methoden können synthetische Lastzeitreihen für unterschiedliche Verbrauchertypen erzeugt werden, die in ihrer Charakteristik nicht von realen Messdaten zu unterscheiden sind, aber gleichzeitig eine weitest gehende Anonymisierung gewährleisten.	Verbesserung der Genauigkeit von Lastzeitreihen, die für weitere Berechnungen dienen; Anonymisierung von Daten
IKT-Sicherheit	**Erkennen von Datenmanipulationen**	
	Mit Hilfe von Datenaggregation und Datenanalysen können Anomalien auch in großen Datenmengen erkannt werden, neuronale Netze können beispielsweise speziell darauf trainiert werden.	Erkennen von Datenmanipulationen, Abwenden von Cyberangriffen zur Erhöhung der Netzsicherheit

Instandhaltung	**Monitoring von HS-Leitungen**	
	Das Monitoring von HS-Leitungen ist ein wichtiger Prozess zum sicheren Betrieb von Freileitungen. Traditionelle Methoden erfordern monatelange Datenerhebung, Datenaufbereitung und manuelle Verarbeitung. Anwendungen mit Satellitendaten und ausgereifte Methoden zur Objekterkennung können dieselbe Aufgabe in Stunden oder Tagen erledigen. Unter Heranziehen historischer Daten werden Zusammenhänge zwischen Abnutzungserscheinungen und Anlagenausfällen hergestellt, die dadurch als Auffälligkeiten erkannt werden können. Typischerweise werden in diesem Bereich Klassifikation, Regression und KNN eingesetzt. In der Praxis werden solche Anwendungen bspw. in Ortsnetzstationen implementiert.	Systemsicherheit, Risikoreduzierung: Vermeidung von Betriebsunterbrechungen, Reduzierung von Gesamtsystemkosten
	Frühwarnsystem für Störungen in Umspannwerken	
	Mitnetz Strom hat auf Basis von Methoden der Künstlichen Intelligenz ein Frühwarnsystem entwickelt, das Störungen in Umspannwerken prognostiziert. Als Ergebnis der Analysen werden Monatsberichte an die verantwortlichen Personen gesendet, die bei Auffälligkeiten rechtzeitig erforderliche Schritte einleiten können.	Vermeidung von Systemausfällen und finanziellen Schäden in beträchtlicher Höhe
	Wartung und Reparatur von Freileitungen	
	Für Wartungs- oder Reparaturarbeiten können Drohnen und Roboter zum Einsatz kommen, die Schwachstellen z.B. durch Verfahren der Bilderkennung anzeigen.	Systemsicherheit, Risikoreduzierung: Vermeidung von Betriebsunterbrechungen
Endkundenbereich	**Flexible Strombedarfsanpassung**	
	KI-gestützte Entscheidungshilfen für mögliche Verbrauchsanpassungen und die Nutzung bzw. den Verkauf von selbst erzeugtem Strom können z. B. auf Basis von Verbrauchs- oder Erzeugungsdaten eines Haushalts generiert und ggf. auch direkt umgesetzt werden.	Flexibler Ausgleich zwischen Angebot und Nachfrage, Verbesserung den Angebots für Kunden

Endkundenbereich	**Stromhandel**	
	Der Handel mit Energie ist bisher meist Profis vorbehalten. Mit maschineller Unterstützung könnte auch für andere Akteure das Interesse an der Börse steigen. Ein selbstlernender KI-Agent ist in der Lage, effiziente Handelsstrategien zu entwickeln und diese gewinnbringend an der Strombörse umzusetzen.	Kostenreduktion, Hürden für Marktteilnehmer reduziert

Tabelle 2: Auswahl an Use Cases, die auf KI- und Datenbasierten Methoden basieren und in den verschiedenen Bereichen des Netzbetriebes bereits zum Teil eingesetzt werden.

2.4 Zusammenfassung

Datengetriebene Prozesse im Umfeld einer kritischen Infrastruktur, wie bei den Stromnetzbetreibern, stellen eine deutliche Herausforderung dar. Insbesondere die Verbindung von Anwendungen auf Basis von Informations- und Kommunikationstechnologie (IKT) für den Betrieb der Stromnetze enthält gefährliche Abhängigkeiten, die adressiert werden müssen. Zum Beispiel kann ein fehlerhafter oder abgebrochener Prozess in einem der beiden Felder kann zu direkten Konsequenzen im jeweils anderen Feld führen, weshalb die datenabhängigen Prozesse, bzw. ihre genutzten Anwendungen, kritisch geprüft und auf ihren Einfluss hin charakterisiert werden sollten.

Eine Einordnungsmöglichkeit wurde in Abschnitt 2.2 aufgezeigt. Hier wird der Netzbetrieb in die Bereiche Netzführung und operative Netzplanung, IKT-Sicherheit, Instandhaltung und Endkundenbereich unterteilt und dazu Kritikalitätsindikatoren (siehe Tabelle 1) definiert. Diese können auf Prozesse in den jeweiligen Bereichen angewendet werden, um abzuschätzen wie kritisch ein Prozess bzgl. seiner negativen Auswirkungen sein kann. Eine allgemeine Abschätzung wurde anhand von Abbildung 2 gegeben.

Abschließend wurde in Abschnitt 222.3 auf die Analyse von Daten insbesondere unter Verwendung von künstlicher Intelligenz (KI) eingegangen. Diese Anwendungen bergen speziell in der Datenverarbeitung und -analyse ein enormes Potenzial bestehende Prozesse zu optimieren bzgl. Geschwindigkeit und Güte, aber können auch komplett neue Anwendungen realisieren, die bisher nicht möglich waren. Eine Übersicht über Anwendungen auf Basis von KI, die einen neuen Nutzen oder Mehrwert mit sich bringen, ist in Tabelle 2 zu finden. Neben den Chancen sind aber auch neue Risiken zu berücksichtigen. Neben den Risiken, die in den Daten und deren Behandlung liegen (siehe Kapitel 3.3), bergen die KI-Anwendungen weitere Risiken bei ihrer Verwendung. Hier wurde auf die Abhängigkeit der Datengrundlage eingegangen sowie auf ein mögliches entstehendes zu hohes Vertrauen in die Ergebnisse der KI und die oft fehlenden Möglichkeiten die Ergebnisse nachzuvollziehen. Dieses liegt einerseits oftmals an dem Black-Box Charakter der KI-Anwendungen, aber auch daran, dass Menschen die Entscheidungen der KI nicht mehr rational nachvollziehen können.

3 Daten als Grundvoraussetzung für Analysen & intelligente Anwendungen im Stromnetz

Wie in Kapitel 2 ausgeführt, bieten KI-basierte Anwendungen neue Möglichkeiten im Netzbetrieb. Diese reichen von verbesserten und effizienteren Prozessen bis hin zu komplett neuen Anwendungen und Ansätzen, die bisher nicht möglich waren (siehe hierzu Tabelle 2 mit einer Auswahl von Anwendungen, die durch die Nutzung von KI-Methoden einen Mehrwert für den Netzbetrieb liefern können). Grundlegende Voraussetzung dafür ist eine hinreichende Datenbasis. Dieser kommt eine besondere Bedeutung zu, da sich die Anwendungen in einem kritischen Umfeld befinden und Fehler in den Ergebnissen oder Ausfälle dieser zu schwerwiegenden Folgen führen können. An der Qualität der Eingangsdaten entscheidet sich bereits die Qualität der Ergebnisse. Weiterhin erweitert und verändert aktuell die Digitalisierung (siehe auch 1.2.1) die analogen Wertschöpfungsketten der Energiewirtschaft hin zu datengetriebener Wertschöpfung, wie beispielsweise Prognoseanbieter. In diesem Rahmen werden Daten zur wertvollen Ressource, aus der durch Auswertungen und Analyseverfahren Mehrwerte für eine effizientere Energieversorgung generiert werden können. Auch die Prozesse der Datenwertschöpfungskette (Generierung → Speicherung → Verarbeitung → Analyse → Verwertung → Löschung) unterliegen dabei Veränderungen. Der Bedarf an neuen Messsystemen und Messstellen und deren Ausbau führen zu einem beschleunigten, exponentiellen Datenwachstum. Diese (neue) Datenbasis ist ein wesentlicher Aspekt in der Transformation des Netzbetriebs hin zur Digitalisierung und Automatisierung herkömmlicher Prozesse. Je höher die Menge an Daten bzw. Informationsdichte und Datenquellen ist, desto höher kann der potenzielle Nutzen der Analysen und Anwendungen sein [12].

In diesem Kapitel wird auf die Erfassung der Daten und deren Quellen sowie auf die Verfügbarkeit und Qualität eingegangen. Da diese Daten die Basis für z.T. neue Prozesse und deren Ergebnisse sowie Maßnahmen im kritischen Umfeld des Netzbetriebes bilden, müssen sie auch bzgl. potenzieller Risiken für den Netzbetrieb analysiert und bewertet werden. Hierzu wurde eine Einordnung in der VNB-Praxis mithilfe von Befragungen und Diskussionen mit Netzbetreibern vorgenommen und unter Kapitel 3.2 beschrieben.

Ziel ist es, ausgewählte Datenquellen im Rahmen der Datenerfassung auf ihren Typ und ihre Verfügbarkeit hin zu charakterisieren und auf die Datenqualität, Datenhaltung sowie deren Übertragung einzugehen. Abschließend werden mögliche Risiken aufgezeigt und Vorschläge wie man Daten schützen kann.

3.1 Wesentliche Aspekte für die Nutzbarmachung und Anwendbarkeit von Daten

Grundsätzlich wird zwischen Stammdaten und Bewegungsdaten unterschieden. Die Stammdaten aller Netzteilnehmer bilden die Grundlage des digitalen Informationsnetzes. Sie enthalten technische Daten sowie Standortdaten von Anlagen und Komponenten bei der Einspeisung bis hin zu Verbrauchern. Bewegungsdaten ergänzen die Datengrundlage mit physikalischen Messwerten z.B. Jahresverbrauchs- und Erzeugungsdaten. Mithilfe der verfügbaren Stamm- und Bewegungsdaten kann ein digitales Abbild des Versorgungsprozesses erzeugt werden.

3.1.1 Datenquellen und Datenerfassung

Für moderne Anwendungen wird eine Vielzahl von Daten aus unterschiedlichen Quellen benötigt. Einige dieser Quellen sind öffentlich und, je nach Anwendung, kostenfrei verfügbar. Andere Quellen liegen nur bestimmten Akteuren vor, können aber im Bedarfsfall zur Verfügung gestellt werden. Weiterhin gibt es noch Quellen, die nicht öffentlich zugänglich sind, aber käuflich erworben werden können und Daten, die das Eigentum einzelner Personen oder Unternehmen sind und nicht käuflich erworben werden können und somit nur von diesen selber verwendet werden dürfen.

Datenquellen

Mit dem Blick auf Anwendungsentwicklungen im Stromnetz liegt ein Großteil der benötigten Daten bei den Netzbetreibern selber. Hierzu zählen beispielsweise Netzmodelle, Anlagendaten und Daten zu Einspeisung und Verbrauch. Für viele Anwendungen werden Wetterdaten bzw. Einspeiseprognosen benötigt. Hier gibt es teilweise frei zugängliche Datenquellen, wie die Online-Plattform renewables.ninja[2], auf der durch Simulationen auf Basis von historischen Satellitenbeobachtungen und Reanalysen Zeitreihen für Windkraft- und Photovoltaikanlagen bereitgestellt werden oder auch kostenlos zur Verfügung gestellte Prognosen vom DWD[3] oder GFS[4]. Alle anderen Wetterdaten, wie z.B. Vorhersagen vom Europäischen Zentrum für mittelfristige Wettervorhersage (ECMWF[5]) müssen, Stand heute, zugekauft werden. Ebenso relevant sind Gebäude- und Energiedaten, die bei den Katasterämtern liegen oder Zensus Daten, z.B. im Rahmen von Berechnungen für die zukünftige Nutzung oder Standortermittlung von Ladesäulen und Wallboxen. Markt-, Wetter- und Geodaten oder auch Daten aus Social-Media-Kanälen erhalten eine signifikante Relevanz, um Verknüpfungen zwischen den einzelnen Datenquellen herzustellen [12].

Seit dem Beginn des Smart Meter Rollouts im Februar 2020 bilden auch Smart Meter Daten eine potentielle Grundlage für Berechnungen zu Verbrauchsprognosen. Smart Meter werden bei Kunden installiert und sind in der Lage den Zählerstand sowie weitere Werte, wie z. B. die Spannung und Frequenz, zu erfassen und zu übermitteln. Um eine sichere Übertragung der Smart Meter Daten zu gewährleisten, wurde speziell ein Smart-Meter-Gateway eingerichtet, das als Kommunikationsplattform die Schnittstelle zwischen Verbraucher und Energiesystem bildet. Das Smart-Meter-Gateway besitzt ein integriertes Sicherheitsmodul, das Daten verschlüsselt übertragen kann und die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik erfüllt. Eine sichere Datenübertragung ist notwendig, da Smart Meter Daten sensible Informationen zu Verbrauchern enthalten, die Rückschlüsse auf die in einem Haushalt lebenden Personen ermöglichen und für unzulässige oder sogar kriminelle Zwecke genutzt werden könnten. Um den Datentransfer solcher Datenmengen möglich zu machen, hat die Bundesnetzagentur seit Dezember 2020 das 450-MHz-Frequenzband vorrangig der Energie- und Wasserwirtschaft zur Verfügung gestellt [31].

[2] https://www.renewables.ninja/
[3] Deutscher Wetter Dienst https://www.dwd.de/DE/Home/home_node.html
[4] US –Wetterdienst https://www.wetterzentrale.de/topkarten.php?model=gfs&time=3&lid=OP
[5] https://www.ecmwf.int/

In Tabelle 3 findet sich eine Übersicht zu häufig genutzten Datenquellen. Als Datenquelle werden hier nicht nur die einzelnen Systeme, sondern auch die Akteure, Anbieter und weitere Arten von Instanzen, bei denen die Daten vorliegen, bezeichnet.

Datenquelle	Datentypen	Öffentlich verfügbar
Netzbetreiber	Asset-/Betriebsmittel-Daten	Nein
	Daten zu Erzeugung und Verbrauch (z.B. Jahresverbrauch Kunden, Lasttypen, Erzeugung von Referenzanlagen, Messdaten usw.)	Nein
	Netzmodelle: • Kenngrößen installierter Betriebsmittel • Ergebnisse Leistungsfluss und-Kurzschlussstromberechnungen • Schaltzustände	Generell nein, aber teilweise werden die Netzmodelle der ÜNB online gestellt im Rahmen der Engpassanalyse[6]
	Geografische Daten/ GIS-Daten	Nein
Netzentwicklungspläne (https://www.netzentwicklungsplan.de/de)	Netzentwicklungspläne mit den Szenariorahmen 2037 / 2045	Ja
DWD	Wetterprognosen und weitere Daten zu Wetterbedingungen	Prognosen frei verfügbar
renewables.ninja (https://www.renewables.ninja/)	Historische Erzeugungsdaten und Wetterbedingungen	Ja
Open Power System Data (https://open-power-system-data.org/)	Historische Erzeugungsdaten und Wetterbedingungen	Ja
NASA's MERRA-2 (https://gmao.gsfc.nasa.gov/reanalysis/MERRA-2/)	Historische Erzeugungsdaten und Wetterbedingungen	Ja
ENTSO-E (https://www.entsoe.eu/data/data-portal/)	Historische Verbrauchsdaten	Ja
Katasteramt	Gebäudedaten (Adresse, Geometrie, Nutzfläche, Baujahr, …)	Nein
Solarkataster	Solarpotenzial	Ja
Geol. Landesamt	Erdwärmenutzung	Nein

[6] https://www.transnetbw.de/de/strommarkt/engpassmanagement/engpass

Schornsteinfeger	Kesseldaten	Nein
Messgerätehersteller	Kenngrößen der Messgeräte, Wechselrichterdaten	Nein
Smart-Meter-Gateway	Smart-Meter-Daten • Zählerstand • Messung elektrischer Größen (Strom, Spannung, Wirkleistung, Frequenz usw.)	Nein
SMARD Strommarktdaten (https://www.smard.de/home)	Stromerzeugung, Stromverbrauch, Großhandelspreise usw.	Ja
Zensus Daten	aktuelle Bevölkerungszahlen,	Ja
	Daten zur Demografie, das heißt Alter, Geschlecht	Ja
	Daten zur Wohn- und Wohnungssituation wie durchschnittliche Wohnraumgröße, Leerstand oder Eigentümerquote	Ja

Tabelle 3: Übersicht einer Auswahl häufig genutzter Datenquellen und deren öffentliche Verfügbarkeit.

Von einigen Unternehmen und der Wissenschaft wird in Deutschland eine fehlende Open-Data-Mentalität beklagt, wodurch die Bereitstellung und Nutzung von Daten oft eingeschränkt ist. In anderen Ländern, wie z.B. der Schweiz, ist die Datengrundlage bereits um einiges besser. In Deutschland unterscheidet sich der Rahmen für die Datennutzung je nach Bundesland. Vorreiterrollen nehmen hier Nordrhein-Westfalen (NRW) und Berlin ein, die eine gute öffentliche Verfügung von GIS-/ GEO-Daten vorweisen können. Um durch Datenhoheit und –Monopole keine Ungleichheiten im Bereich des Netzbetriebes zu erzeugen, ist es wichtig, dass möglichst viele relevante Daten für den Netzbetrieb offen zur Verfügung stehen. Es sei aber angemerkt, dass bestimmte strukturelle und personifizierte Daten unbedingt geschützt bleiben müssen.

Datenerfassung

Grundlage für die Datenerfassung sind Zähl- und Messeinrichtungen, aus denen die Rohdaten über Kommunikationsgeräte mit speziellen Protokollen in ein Datenerfassungssystem übertragen werden. Hierfür werden Anlagen mit Sensorik ausgestattet, die verschiedene Parameter erfassen können und diese über eine Funk- oder Netzwerkverbindung übermitteln. Bei der Datenerfassung kann zwischen strukturierten und unstrukturierten Daten unterschieden werden. Klassisch strukturierte Daten stellen z.B. Messwerte einer Erzeugungsanlage dar, die anhand des Inhalts und Formats eindeutig bestimmbar sind. Unstrukturierte Daten umfassen Daten in Form von Texten, Bildern oder Audio- und Videodaten [12]. Generell gibt es verschiedene Datenmodelle für die

Beschreibung von Mess- und Anlagendaten auf diese abgebildet werden können (z.B.: IEC61850 oder CGMES). Siehe hierzu auch den nächsten Abschnitt 3.1.2.

Zusätzlich können Daten zu Kunden oder Lieferanten sowie Daten aus Geschäfts- und Managementprozessen die Datengrundlage ergänzen. Eine Beschreibung zu den verschiedenen Datenarten und wie sie unterschieden werden können findet sich im Gutachten „Digitale Marktkommunikation für das Energiesystem der Zukunft“ [37] der dena.

> *Eine umfassende Datenerfassung stellt den ersten Schritt in Richtung Digitalisierung dar. Ein hoher Grad an Digitalisierung ist dann erreicht, wenn eine weitgehend automatisierte Datenerfassung erfolgt.*

3.1.2 Standardisierte Schnittstellen und Datenformate

Für eine gemeinsame Nutzung und Vernetzung untereinander spielt das Format der Daten eine große Rolle. Um Entwicklungen flächendeckend nutzen zu können, müssen die Daten in einheitlichen, möglichst standardisierten Formaten vorliegen, um eine langwierige Datenaufbereitung und individuelle Anpassungen zu vermeiden. Die Nutzung von standardisierten Datenmodellen, welche in der Regel eine Beschreibung beinhalten, welche Daten wie zu beschreiben sind und in welchen Format diese dargestellt werden sollen, lässt auch eine genauere Prüfung der Daten auf Vollständigkeit und Qualität zu und erleichtert somit außerdem die Validierung der Daten.

Für Übertragungsnetzbetreiber gibt es bereits verpflichtende Vorgaben. In der 2015 erlassenen CACM Verordnung wurde ein europaweiter CGMES-Implementierungsleitfaden für Übertragungsnetzbetreiber festgelegt [27]. Hierdurch muss jeder europäische ÜNB ein Einzelnetzmodell im CGMES Format zur Verfügung stellen [32]. CGMES bezeichnet die „Common Grid Model Exchange Specification“, die auf den CIM (Common Information Model) Standards IEC 61970 und weiteren basiert und von der ENTSO-E entwickelt wurde [29]. Dieses Format dient als Standard für den Austausch von Netzmodelldaten, in die technischen Eigenschaften, wie z. B. die Topologie eines Stromnetzes, beschrieben werden. In Deutschland wird CGMES auch durch Hochspannungsnetzbetreiber im Rahmen der GLDPM zum Datenaustausch mit den ÜNBs eingesetzt. Eine solche verpflichtende Vorgabe wäre auch für die Mittelspannungsebene/ niedrigere Spannungsebenen denkbar. Hier gibt es bereits einen Vorschlag für ein CDPSM Modell (Common Distribution Power System Model), was im Gegensatz zu CGMES weitere Spezifika von Verteilnetzen umfasst [30]. Grundlegend standardisierte Schnittstellen und Formate existieren bereits, eine detaillierte Übersicht dazu findet sich in der dena-Analyse „Schnittstellen und Standards für die Digitalisierung der Energiewende“ [35].

Eine Schwierigkeit stellt die Synchronisation von verschiedenen Datenquellen und Anwendungen dar. Verschiedene Prozesse bauen auf den gleichen Daten auf, beispielsweise sind digitale Netzmodelle die wichtigste Grundlage für die operative Netzplanung, im Falle der Bewertung von Anschlussgesuchen dienen diese aber auch als Grundlage für die strategische Netzplanung. Beide Prozesse stellen unterschiedliche Anforderungen an die Nutzung und Verarbeitung der Daten. Diese verschiedenen Anforderungen führen häufig zu einer doppelten Datenhaltung, da getrennte Anwendungen für jeden Prozess entwickelt und gepflegt werden, was einen hohen Aufwand zur Folge haben kann. Anschlussgesuche werden beispielsweise in Excel- oder GIS-basierten Anwendungen bearbeitet wohingegen die Zielnetzplanung mit Netzberechnungsprogrammen

wie DIgSILENT PowerFactory, NEPLAN oder PSS SINCAL erfolgt [34]. Abhilfe kann in bestimmten Fällen eine zentrale Datenplattform[7] schaffen, die eine konsistente Datenhaltung für verschiedene Anwendungsfälle ermöglicht [34].

> *Standardisierte Schnittstellen, Datenmodelle und Prozesse an den Netzverknüpfungspunkten nehmen einen wichtigen Stellenwert ein und dienen als Grundlage für einen transparenten Informationsaustausch zwischen den Netzbetreibern. Zudem ermöglichen sie eine effiziente Steuerung, einen effizienten Netzbetrieb und die Möglichkeit einer koordinierte Erbringung von Netz- und Systemdienstleistungen [11]. Neben standardisierten Datenformaten nimmt eine zentrale Datenhaltung eine bedeutende Rolle ein. Aufgrund der zunehmenden Komplexität des Energiesystems werden zentrale Datenplattformen notwendig sein, da die heute oft genutzten dezentralen lokalen Dateisysteme nicht geeignet sind, um die zunehmend vernetzten Energiesysteme zu planen und zu betreiben. Sind alle Daten an zentraler Stelle verfügbar, wird die Verknüpfung der einzelnen Daten vereinfacht und die Möglichkeiten für deren Nutzung steigen.*

Auch im Rahmen des Redispatch 2.0 wurden in gemeinsamen Projekten von Übertragungs- und Verteilnetzbetreibern Plattformlösungen erarbeitet, um einheitliche Regeln und Formate zum Datenaustausch zu schaffen (DA/RE, Connect+) [33].

3.2 Datenverfügbarkeit und Datenqualität – Einordnung in der VNB-Praxis

Nach der Datenerfassung spielt das Kriterium der Datenverfügbarkeit eine wichtige Rolle. Die **Datenverfügbarkeit** beschreibt, ob der Zugang zu den Daten dauerhaft gewährleistet und geregelt ist, sodass diese für Anwendungen genutzt werden können. Ebenso essenziell ist die **Datenqualität**. Der Begriff Datenqualität beschreibt eine vollständige Datenerfassung sowie die Richtigkeit und Verlässlichkeit der Dateninhalte. Im Rahmen einer **Datenvalidierung** muss eine Plausibilisierung der Daten erfolgen, bei der geprüft wird, ob alle Daten noch aktuell sind oder sich Veränderungen ergeben haben, für die die Daten nicht mehr aussagekräftig sind. Im Laufe der Zeit ändert sich beispielsweise das Verhalten oder der Typ von Verbrauchern und somit die Standardlastprofile. Profile, die vor Jahren den Zustand noch gut abgebildet haben, sind heute teilweise nicht mehr repräsentativ, da sich insbesondere durch den Einzug der Elektromobilität und der vermehrten Verwendung von Wärmepumpen das Verhalten geändert hat. Nicht zuletzt durch Corona haben sich in den letzten Jahren signifikante Änderungen des Verbrauchverhaltens ergeben, z.B. durch die überwiegende Arbeit im Home-Office. KI-Entwicklungen, die Lastprofile automatisiert flexibel an solche kurzfristigen Änderungen anpassen können, würden hier einen großen Mehrwert bieten.

---

[7] **Beispiel einer zentralen Datenhaltung**
In Zusammenarbeit mit verschiedenen Netzbetreibern wird derzeit z.B. an einer Netzdatendrehscheibe gearbeitet, die eine zentrale Plattform zur Datenbereitstellung für andere Systeme bieten soll. Diese Plattform basiert auf der Software pandapower, die Lastfluss- oder Kurzschlussberechnungen sowie Zeitreihensimulationen ermöglicht. Voraussetzung hierfür sind rechenfähige Netzdaten, die auf der Plattform abgelegt werden. Neben Netzdaten können aber auch beliebige andere Daten, wie z.B. Störungsdaten, hinzugefügt und mit den Netzdaten verknüpft werden. Für die geplante Datendrehscheibe wird eine Datenbanktechnologie mit einer vorgelagerten API angestrebt, über die standardisierte Zugriffsmöglichkeiten auf die abgelegten Daten sowie das Hinzufügen neuer Daten geregelt wird. Die API ermöglicht es Netzbetreibern auch selbst gezielt Daten auszuspielen. Realisiert wird die neue Open-Source-Datenbank mit der Datenbanktechnologie NoSQL [34]. „Ein weiteres Ziel der Datenplattform ist es, die Datenhaltung und vorgelagerte Prozesse wie die Authentifizierung und Datenvalidierung derart zu abstrahieren, dass der Nutzer sich nicht mit der Funktion der Datenplattform auseinandersetzen muss, sondern ganz auf die Nutzung der Daten konzentrieren kann. Beim Einspielen von Daten werden diese validiert und der Nutzer im Falle von Inkonsistenzen darauf hingewiesen. Ein umfangreiches Authentifizierungssystem ermöglicht dabei eine flexible Zugriffskontrolle, was besonders für Anwendungen für und bei Netzbetreibern und frei im Internet verfügbaren Anwendungen essenziell ist. [34]"

Zur Sicherung der Qualität können ebenfalls KI-Verfahren eingesetzt werden, um Anomalien in der Datengrundlage zu erkennen, bevor die Daten in anderen Anwendungen genutzt werden. Eine zuverlässige Datenverfügbarkeit und hohe Datenqualität sind wesentlich für spätere Anwendungen, da sowohl der Erfolg als auch die Qualität der Anwendung von der Verfügbarkeit und Qualität der Daten abhängt. Kann der Datengrundlage nicht vertraut werden, kann auch der Anwendung in Folge nicht vertraut werden.

3.2.1 Hürden für Datenverfügbarkeit und –qualität in der VNB-Praxis – Einordnung[8]

Verfügbarkeit der Daten

Prinzipiell liegt ein Großteil der erforderlichen Daten bei den Netzbetreibern vor. An vielen Stellen müssen aber noch Hürden überwunden werden, bis die Daten zur Nutzung für datengetriebene KI-Anwendungen bereitgestellt werden können. So können beispielsweise die Daten selbst zwar im Quellsystem vorhanden sein, aber ein Export der Daten in Zielsysteme ist nicht möglich oder sehr aufwendig, was eine Nutzung in Anwendungen erschwert oder unmöglich macht. Dies liegt zum Teil an unzureichender oder fehlerhaften Dokumentation der Daten aber auch an unterschiedlichen Formaten, die durch zum Teil historische Änderungen in der verwendeten Software begründet sind.

Für ein solides Training der KI und aussagekräftige Ergebnisse sind in der Regel viele Eingangsdaten in hoher zeitlicher Auflösung über einen langen Zeitraum notwendig. Durch veraltete Messtechnik kann nur ein Teil der eigentlich benötigten Größen erfasst werden, z.B. bei Schleppzeigern, die vielerorts noch genutzt werden und keine Möglichkeit zur Richtungsangabe besitzen und auch nur den maximalen Wert innerhalb des Ablesezeitraumes angeben. Auch das Ableseintervall von Daten, die nach wie vor nur analog vorliegen und bei denen eine händische Ablesung teils nur einmal jährlich erfolgt, wie z.B. der jährliche Stromverbrauch eines Kunden, ist nicht ausreichend. Hinzu kommen fehlende Messwerte sowie dass die Datenvollständigkeit nicht immer gewährleistet ist.

Aktualität der Daten

Neben veralteter oder zu wenig Messtechnik liegt ein weiteres Problem in der Nutzung veralteter Daten an sich. Diese können für aktuelle Anwendungen nicht mehr gültig sein. Als Beispiel können hier veraltete Netzpläne genannt werden, in denen die Lasten aus Netzmodellen von z.B. 2010 oder 2012 stammen und die für aktuelle Berechnungen lediglich skaliert werden, bis sie mit den Transformatorwerten annähernd übereinstimmen. D.h. man skaliert und aggregiert die Lasten, bis sie bei einem bestimmten Gleichzeitigkeitsfaktor die abgelesenen Messwerte am Transformator repräsentieren. Der Grund hierfür ist ein intransparentes Lastverhalten, Einspeisungen hingegen sind besser bekannt. Darüber hinaus werden für Berechnungen stellenweise geschätzte Daten, sogenannte Pseudomessungen, verwendet, bei denen aber unklar ist in welchem Umfang sie von der Realität abweichen, da sie nicht anhand echter Messungen validiert werden, sondern nur in

[8] Die Einordnung erfolgt auf Basis von Erfahrungswerten aus verschiedenen Forschungsprojekten der letzten 5 Jahre sowie durch direkte, für diesen Zweck geführte Befragungen einer Auswahl von VNB. Da durch die Energiewende aktuell insbesondere die Verteilnetze von Veränderungen betroffen sind und diese Netze in der Mittel- und Niederspannung (aktuell noch) ungenügend ausgemessen sind, wird an dieser Stelle die aktuelle Datenverfügbarkeit deutscher Verteilnetzbetreiber betrachtet, mit Fokus auf kleinere Hochspannungsnetzbetreiber sowie Mittel- und Niederspannungsnetzbetreiber.

aggregierter Form oder im Zusammenspiel mit weiteren Messungen plausibilisiert werden können (z.B. durch Messungen an Umspannwerken). Exakte Berechnungen sind unter diesen Umständen schwierig bis unmöglich.

Konsistenz der Daten

Eine der größten Hürden zur Erstellung einer für KI-Anwendungen benötigten Datenbasis ist die Verknüpfung der einzelnen Daten. Meist werden Daten aus verschiedenen Systemen benötigt, z.B. aus GIS- und Asset-Datenbanken, Prognosesystemen, Prozess- oder Leitsystemen. Die Verknüpfung dieser unterschiedlichen Daten ist aber oft schwierig und nur mit hohem Aufwand zu erreichen, da es sich um unterschiedliche Datenmodelle handelt, die nicht konsistent sein müssen und zum Teil auch unterschiedliche Geschäftsbereiche bei Energieversorgern und Netzbetreibern beschreiben. Zudem müssen einige Daten erst manuell aufbereitet werden, bevor sie genutzt werden können, wie beispielsweise Netzmodelle in denen neu installierte Leitungen fehlen.

> *Insgesamt sind die Datenmenge und vor allem die Datenqualität im Bereich der Stromverteilnetze in der Mittel- und Niederspannung im Status quo ungenügend. Gerade Echtzeitdaten stehen sowohl in der Mittel- als auch Niederspannung nicht ausreichend für eine aktive oder automatisierte Betriebsführung zur Verfügung. Allgemein ist, unabhängig vom Datentyp, die Datenvollständigkeit und Datenqualität umso geringer, je niedriger die Spannungsebene ist. Besonders in der Niederspannung erfolgt partiell noch gar keine (Echtzeit-Mess-) Datenerfassung. Damit Netzbetreiber das ihnen zur Verfügung stehende Potenzial zukünftig voll ausschöpfen können, ist es wichtig, dass sie sich bereits jetzt mit dem Datenbestand innerhalb des Unternehmens auseinanderzusetzen und die Datengrundlage ggf. verbessern.*

Expertise und Personal

Die nächste Hürde bei der Einführung und Entwicklung von datengetriebenen Anwendungen liegt im fehlenden Know-How und der Erfahrung. Vor allem bei kleineren Netzbetreibern, die keine eigene Entwicklungsabteilung betreiben können, fehlt die Expertise darüber in welchen Bereichen und auch in welchen Datenformaten eine Datensammlung und -archivierung überhaupt sinnvoll ist. Und auch dies führt wieder zur nächsten Schwierigkeit für eine flächendeckende Einführung von innovativen Lösungen: Der Mangel an Ressourcen. Weder ist Personal mit dem entsprechenden Know-How in ausreichender Anzahl verfügbar noch die finanziellen Mittel für Personal und Messtechnik. Auch wenn durch innovative Methoden Messstellen eingespart werden können, muss doch an einigen Punkten eine Umrüstung z.B. von veralteten Ortsnetzstationen zu fernsteuerbaren Stationen stattfinden, was in der Umsetzung und Wartung Kosten verursacht.

> *Angemerkt sei hier, dass nicht alle KI-Anwendungen Umbaumaßnahmen durch Erweiterung der Messtechnik im Netz erfordern. Zudem haben viele neue Anwendungen auch das Potenzial durch deren Einsatz Kosten einzusparen oder Investitionen zu amortisieren. Zum Beispiel können, in Verbindung mit einer KI-basierten Zustandsschätzung für die Mittelspannung, optimale Standorte für weitere Messstellen ermittelt werden, wodurch eine effiziente und kostenminimierte Ausstattung mit neuer Technik möglich ist[9]. Werden diese Verfahren großflächig eingesetzt, sind zukünftig höhere Beobachtungsmöglichkeiten in der Mittel- und*

[9]Ein Use Case unter Verwendung dieser Methode wurde auch im praktischen Teil des Data4Grid Projekts in einer Challenge bearbeitet (siehe auch *Challenge 2: Evaluierung relevanter Messstellen zur Erhöhung der Netztransparenz* im Data4Grid Projektbericht).

Niederspannung zu erwarten. Dies wird mit Hinblick auf die steigende Zahl von E-Kfz oder einer potenziellen Erweiterung des Redispatch 2.0-Prozesses in Richtung Niederspannung notwendig sein.

Abschließend lassen sich folgende Erkenntnisse formulieren:

Damit Netzbetreiber das ihnen zur Verfügung stehende Potenzial voll ausschöpfen können, ist es wichtig, dass sie sich bereits jetzt mit dem Datenbestand innerhalb des Unternehmens auseinandersetzen und die Datengrundlage verbessern. Ein einmaliger, vertretbarer Initialaufwand kann bereits Möglichkeiten schaffen, langfristig zu profitieren. Grundlegende Schritte können hierbei sein:

- *Fehlerkorrekturen: Die digitale Netztopologie prüfen und ggf. überarbeiten, d.h. beispielsweise fehlende oder falsch zugeordnete Betriebsmittel ergänzen, um ein rechenfähiges Netzmodell zu erhalten.*
- *Schalterstellungen dokumentieren.*
- *Vorhandene Daten verknüpfen (SAP, GIS, …), ggf. durch Einbindung externer Daten (Gebäudeinformationen, Umgebungsinformationen, sozio-demographische Daten).*
- *Internes Know-How aufbauen und pflegen.*

3.3 Datenbasierte Risiken und Datenschutz

Wie in Kapitel 2 beschrieben bergen datengetriebene Anwendungen, speziell unter Verwendung von KI-Verfahren, verschiedene Risiken insbesondere bei Anwendung in kritischen Infrastrukturen. Neben dem Aspekt, dass die verwendeten Informationen korrekt und für die Anwendung passend sein müssen, ergibt sich gerade bei der Verwendung von KI eine erhöhte Abhängigkeit von der Datengrundlage. Weitere Risiken stellen ein zu hohes Vertrauen in die Ergebnisse sowie eine oftmals fehlende Möglichkeit, die Entscheidungsfindungen bzw. die Ergebnisse von KI-Anwendungen nachzuvollziehen dar, da diese oft eine Black-Box darstellen (siehe 2.3.1).

Nicht nur die Verwendung von datengetriebenen Prozessen und Anwendungen kann Risiken enthalten, sondern auch schon die Haltung der Daten und deren Übertragung an interne und externe Systeme können Risiken darstellen. Zusätzlichen bergen die Daten selbst das Risiko manipuliert zu werden und führen somit bei Ihrer Nutzung zu manipulierten Ergebnissen. Im Folgenden wird auf diese datenbasierten Risiken eingegangen und auch auf mögliche Schutzmaßnahmen.

3.3.1 Datenhaltung

In Kapitel 3.1 wurde bereits kurz auf die Art der Datenhaltung eingegangen. In der Regel findet diese in bestimmten (zum Teil standardisierten) Datenformaten in Datenbanken statt. Hierbei kann man allgemein zwischen zentraler und dezentraler Datenhaltung unterscheiden. Beide bieten Vor- und Nachteile und bringen ihre eigenen Risiken mit. Im Folgenden werden diese beiden Ansätze kurz beschrieben und die jeweiligen Vorteile sowie Nachteile bzw. Risiken aufgezählt.

Zentrale Datenhaltung

Bei der zentralen Datenhaltung werden die Daten von einem Anbieter (intern oder extern) über eine Schnittstelle (z.B. URL für REST) durch eine Datenplattform zur Verfügung gestellt. Die Daten werden von dem Anbieter gewartet, gepflegt und gesichert. Der Anbieter sollte sicherstellen, dass die ein- und ausgehenden Daten nur von authentifizierten Benutzern oder Anwendungen abgerufen oder gesendet werden dürfen. Die Datenplattform sollte von dem Anbieter, der zentralen Struktur, resilient und skalierbar zur Verfügung gestellt werden.

Die Daten können dann beispielsweise über eine REST-Schnittstelle gesendet oder empfangen werden. Über einen API-Key und/oder OAuth 2.0 wird ein Benutzer identifiziert und die richtigen Berechtigungen erteilt. Mit Hilfe verteilter Datenbanktechnologie (z.B. MongoDB) und Virtualisierungen (z.B. Docker) kann eine resiliente und hochskalierbare Datenplattform entstehen. Dieser Ansatz hat z.B. die Vorteile, dass

- der Zugang und das Format eindeutig durch den Anbieter beschrieben sind und somit nicht unterschiedliche Formate verwendet werden.
- der Anbieter eindeutig die Expertise und Erfahrung sicherstellen kann, die für das Betreiben solch einer Plattform notwendig ist.
- durch die hohe Expertise des Plattformbetreibers Skalierbarkeit, Resilienz und Authentifizierung der Zugänge sichergestellt werden.

Dieser Ansatz bietet aber auch Nachteile in Form von den Risiken, dass

- ein einziger Anbieter leichter durch Cyberangriffe korrumpiert werden kann und Daten von vielen Kunden (VNBs und ÜNBs) gestohlen werden können.
- der Anbieter selbst auf eine Vielzahl von hochkritischen Daten zugreifen könnte und man diesem vertrauen muss.

Dezentrale Datenhaltung

Bei dem dezentralen Ansatz werden die Daten von unterschiedlichen Anbietern sowie VNBs und ÜNBs zur Verfügung gestellt. Jeder (Daten-)Anbieter hat einen eigenen Zugangspunkt über den die Daten empfangen und gesendet werden können. Dabei können unterschiedliche Zugriffstechnologien (z.B. REST, SFTP etc.) verwendet werden.

Hierbei müssen sich die (Daten-)Anbieter (z.B. VNBs und ÜNBs) darüber einigen den Datenaustausch über ein bestimmtes Format (z.B. CGMES) erfolgen zu lassen. Die VNBs und ÜNBs stellen nun über unterschiedliche Zugänge (SFTP, REST etc.) die Daten zur Verfügung. Jeder dieser Anbieter betreibt sein eigenes Rechenzentrum und verwendet dazu unterschiedliche Technologien.

Die Vorteile dieses Ansatzes lassen sich u.a. durch folgende Punkte zeigen:

- Eine hohe Anzahl an Anbietern mit verschiedenen Technologien kann schwieriger durch Cyberangriffe korrumpiert werden.
- Sollte ein Anbieter korrumpiert werden, wird eine geringere Anzahl an Daten gestohlen.
- Die Daten verbleiben (lokal) bei den VNBs und ÜNBs.

Die Nachteile dieses Ansatzes sind u.a., dass

- es keinen eindeutigen Zugangspunkt gibt, womit erst festgestellt werden muss, wer welchen Zugangspunkt betreibt.
- jedes Unternehmen eigene Experten einstellt und ein eigenes Rechenzentrum betreibt.
- unterschiedliche und verschiedene Technologien für die Bereitstellung der Daten verwendet werden können. Somit kann ein höherer Entwicklungsaufwand entstehen.

Durch diesen erhöhten Aufwand entsteht außerdem das Risiko, dass nicht genügend Expertise bei den jeweiligen VNBs und ÜNBs vorliegt (durch z.B. fehlendes Fachpersonal) wodurch veraltete, unsichere Technologien verwendet werden können oder auch aktuelle Technologie nicht richtig eingesetzt wird und dadurch Sicherheitsrisiken entstehen.

> *Eine zentrale Datenplattform, die von einem Anbieter zur Verfügung gestellt wird ist deutlich einfacher zu betreiben und zu warten. Es ist eine geringere Anzahl an Know-How (Experten) und Infrastruktur (Rechenzentren) notwendig, als wenn jeder Netzbetreiber seinen eigenen Zugang zur Verfügung stellt. Selbst wenn auf einem Standard wie CGMES gesetzt wird, ist nicht eindeutig bestimmt wie Daten zur Verfügung gestellt werden. Auch das Datenmodell lässt unterschiedliche Interpretationen und Auslegungen zu. Datensicherheit ist ein sehr wichtiger Bestandteil im Netzbetrieb und eine dezentrale Bereitstellung der Daten kann die Sicherheit erhöhen. Sollte jedoch nicht genügend Expertise bei den Netzbetreibern vorhanden sein, können veraltete Technologien verwendet werden oder die eingesetzte Software wird fehlerhaft parametriert. Dies kann dann ein Sicherheitsrisiko darstellen. Möglich wäre auch ein Hybridsystem mit einem Zugangspunkt, der entsprechende Weiterleitungen zu den Datenquellen, die bei den Netzbetreibern in Betrieb sind, vornimmt.*

3.3.2 Datenschutz und Datenübertragung

Das Risiko eines datengetriebenen Netzbetriebs liegt u.a. in dem Austausch der Daten zwischen verschiedenen Netzbetreibern (speziell netzebenenübergreifend) sowie mit externen Partnern. Werden Daten übertragen besteht immer das Risiko, dass bei dieser Übertragung die Daten abgegriffen, manipuliert (gewollt oder auch ungewollt) oder auch zerstört werden. Letzteres kann durch eine redundante Datenhaltung minimiert werden, kann aber dennoch dazu führen, dass ein wichtiger Prozess zumindest kurzfristig unterbrochen wird. Potenziell gefährlicher sind die Risiken, dass Daten abgegriffen und/oder manipuliert werden.

Manipulation kann auch ungewollt, ohne den Eingriff Dritter passieren, wenn z.B. die Datenverbindung fehlerhaft ist und sich die ursprünglichen Daten verändern. Dieses führt in der Regel zu deutlichen Auffälligkeiten, die schnell erkannt werden können. Ist das aber nicht der Fall, können sich z.B. die Werte in Messungen oder Sollwerten ändern, was dann schwerwiegende Folgen haben kann. Bei einer aktiven Manipulation ist ein Erkennen der veränderten Daten deutlich schwieriger, da die Manipulation einen bestimmten Zweck erfüllen und in der Regel nicht durch Auffälligkeiten bemerkt werden soll.

Ein Abgreifen bzw. Stehlen von Daten hat erstmal keine unmittelbaren Folgen, da der betroffene Prozess nicht unterbrochen wird und es auch zu keiner Änderung der Daten kommt. Die Folgen

können aber im Nachhinein drastisch ausfallen, wenn z.B. Netzdaten in Form von Topologie- oder Betriebsmittelinformation erbeutet werden. Mit diesen lassen sich dann z.B. Schwachstellen im Netz und mögliche Angriffsziele identifizieren.

Datensicherheit und Datenschutz

Bei der Nutzung von Daten gilt es verschiedene Aspekte im Rahmen des Datenschutzes und der Datensicherheit zu beachten. Die Datensicherheit umfasst den Schutz aller Arten von Daten im Bereich der Datenerhebung, Datenübertragung, Datenverarbeitung, Datenspeicherung sowie der Datennutzung [24]. Speziell befasst sich die Datensicherheit mit den technischen und organisatorischen Maßnahmen, die umgesetzt werden müssen, um Daten zu schützen. Sicherheitsrisiken bestehen u.a. durch technische Mängel oder einen fremden Zugriff auf Daten, was insbesondere durch die digitale Vernetzung über das Internet von Bedeutung ist [41]. Ziel ist es Sicherheitsrisiken zu begegnen und Daten vor Manipulationen, Verlust oder unberechtigtem Zugriff zu schützen [42]. Die Schutzziele können in die drei Kategorien Vertraulichkeit, Integrität und Verfügbarkeit unterteilt werden [45].

Unter **Vertraulichkeit** wird verstanden, dass der Zugriff auf Daten nur von befugten Personen vorgenommen werden kann. Die unbefugte Informationsgewinnung wird als Angriff auf die Vertraulichkeit gesehen. Zur Wahrung der Vertraulichkeit müssen Sicherheitsmaßnahmen ergriffen werden, durch die ein unbefugter Zugang sowohl zu gespeicherten als auch zu übermittelte Daten verhindert werden kann [42].

Integrität steht für korrekte, unveränderte und verlässliche Daten, d.h. dass Daten nicht manipuliert oder durch technische Defekte verändert sind. Tritt eine Verfälschung der Daten auf, d.h. enthält der Empfänger andere Informationen als die, die vom Sender geschickt wurden, liegt eine Verletzung der Integrität vor. Neben absichtlichen Angriffen auf den Inhalt von Daten können Software- oder Hardwarefehler zu falschen Ergebnisse bzw. Informationen führen [42].

Verfügbarkeit bedeutet, dass vorhandene Daten und Systeme im Bedarfsfall für autorisierte Personen zur Verfügung stehen. Durch einen Serverausfall oder Ausfall von Kommunikationsmitteln kann eine Unterbrechung der Verfügbarkeit erfolgen.

> *Die Datensicherheit spielt in der Energiewirtschaft bei datengetriebenen Prozessen bzw. Anwendungen eine besonders große Rolle, da die Verlässlichkeit der Dateninhalte sowie die Datenverfügbarkeit maßgeblich für deren Output ist. Die Einhaltung der drei Schutzziele ist wesentlich für eine erfolgreiche Nutzung von datengetriebenen Anwendungen und der Ausschöpfung des durch die Digitalisierung zur Verfügung stehenden Potentials.*

Sicherer Datenaustausch

> *Für die Nutzung von Daten aus verschiedenen Systemen ist es in den meisten Fällen unabdingbar, dass ein Datenaustausch stattfindet, um diese in den Zielsystemen verknüpfen zu können. Der Datenaustausch kann innerhalb eines Unternehmens zwischen verschiedenen Systemen stattfinden oder außerhalb mit externen Partnern bzw. Drittanbietern. Unter Berücksichtigung der kritischen Prozesse im Stromnetz stellt die Datenübertragung ein direktes Risiko dar und ist selbst als kritisch anzusehen, weil bei einer Unterbrechung, Manipulation oder Ausfall der Übertragung wichtige Informationen nicht mehr verfügbar sind und das direkte Auswirkungen auf die Prozesse in der kritischen Umgebung des Netzbetriebes haben kann. Besonders Schnittstellen, an*

denen Daten von einem System zum anderen übertragen werden, können eine Schwachstelle sein und ein Sicherheitsrisiko darstellen. Hier könnten während der Datenübertragung durch ungewollten Zugriff Daten abgefangen werden. Um die Datenübertragung möglichst sicher zu gestalten, können verschiedene Vorkehrungen getroffen werden.

Die moderne Informationstechnologie (IT) bietet verschiedene Möglichkeiten, um die Datenübertragung abzusichern und ungewollte Zugriffe zu verhindern. Über Authentifizierungs-Methoden kann der Zugriff auf verschiedene Datenbereiche für unterschiedliche Nutzer eingeschränkt werden. Darüber hinaus können Daten verschlüsselt übertragen werden (z.B. SSL). Eine Beschränkung des Zugriffs kann auch auf der Vermittlungsschicht stattfinden z.B. durch eine IP-White- bzw. Blacklist.

Als zentraler Speicherort für einen Datenaustausch werden zunehmend Datenbanken genutzt, die entweder intern auf eigenen Servern eines Unternehmens liegen oder auch als Cloudanwendung betrieben werden. Die Cloud-Nutzung kann allerdings ein höheres Risiko darstellen, da die eigentliche Software nicht vor Ort oder in Deutschland, sondern auf Servern weltweit, z.B. in den USA oder China, laufen kann und es somit größere, komplexere Übertragungswege gibt, die potenzielle Angriffsflächen darstellen können, aber auch die dortige Gesetzgebung anders und zum Teil weniger streng ist als die Deutsche. Allerdings ist auch bei nationalen Anbietern nicht unbedingt von kürzeren Kommunikationswegen auszugehen. Weiterhin haben externe Unternehmen prinzipiellen Zugriff auf die Daten und der Kreis der Datenverantwortlichen ist dadurch vergrößert. Daher sind für Daten-Clouds genaue Sicherheitsvorkehrungen nötig, um das nötige Sicherheitsmaß zu erreichen. Um die Daten in einer Datenbank zu schützen, können verschiedene Verfahren angewendet werden: Benutzer und Rollendefinition für die Authentifizierung, SSL für die Datenübertragung von und zur Datenbank und spezielle Spaltenverschlüsselungstechnik der jeweiligen Datenbanksysteme und Festplattenverschlüsselung. Grundsätzlich ist es empfehlenswert bei einem Datenaustausch Schnittstellen wie z.B. REST über https oder für Dateiaustausch einen sftp-Server zu nutzen, über den eine verschlüsselte Übertragung stattfinden kann. Hierdurch wird verhindert, dass im Fall von unberechtigten Datenabgriffen ein Nutzen aus den Daten gezogen werden kann.

Trotz diverser Sicherheitsmaßnahmen können Sicherheitslücken auftreten und beispielsweise API-Keys oder Benutzerzugänge gekapert werden. Einen 100%igen Schutz kann kein Verfahren gewährleisten. Vor allem müssen Sicherheitsmaßnahmen kontinuierlich aktualisiert werden, da mit der Weiterentwicklung der Computertechnologien auch die Möglichkeiten für Angriffe steigen.

3.3.3 Datenmanipulation

Datengetriebene Prozesse bieten nicht nur eine Angriffsfläche für Hackerangriffe, die das Ziel haben z.B. Betriebsmittel auszuschalten, um einem Stromausfall zu erzielen, sondern auch für weitere Datenmanipulationen, die bestimmte Vorgänge oder Prozesse herbeizuführen sollen.

Besonders künstliche neuronale Netze sind anfällig für diese Art von Attacken, sogenannte „Adversarial Attacks“. Bei Adversarial Attacks werden die Eingangsdaten durch leichte, aber sehr geschickte Veränderung derart manipuliert, dass das neuronale Netz getäuscht und die Ergebnisse

verändert werden. Wie solche Manipulationen aussehen können, kann am Beispiel der Bilderkennung gezeigt werden, die häufig als KI-Methode genutzt wird. In Abbildung 3 ist ein herkömmliches Stoppschild zu sehen. Im „sauberen" Zustand wird es von einer KI als Stoppschild erkannt. Durch Verschmutzungen wie Farbe oder Aufkleber, kann es fehlerhaft als ein anderes Schild identifiziert werden, was z.B. für das autonome Fahren gravierende Auswirkungen hätte.

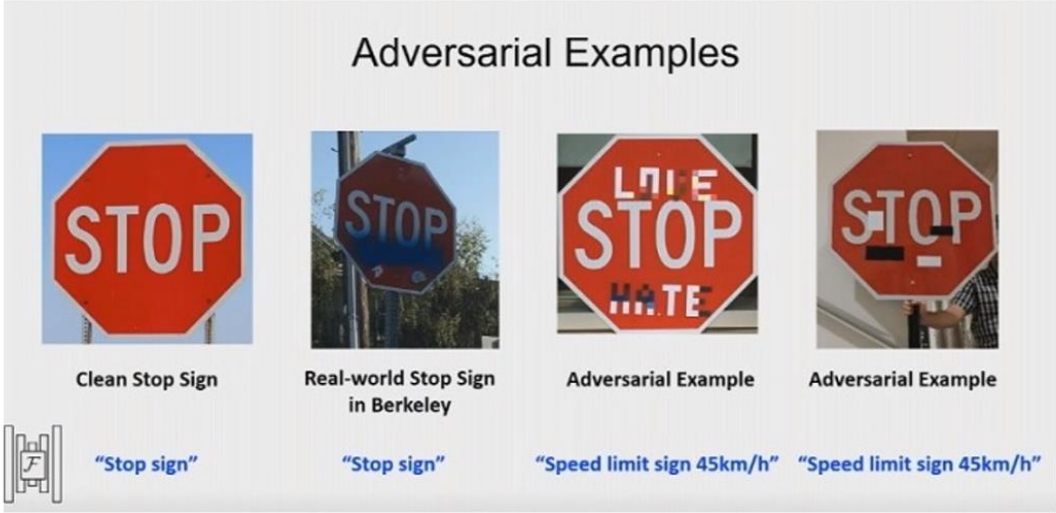


Abbildung 3: Manipulationsmöglichkeiten von Daten bei Anwendungen mit Bilderkennungsverfahren. (Quelle: Dawn Song, AI and Security: Lessons, Challenges and Future Deirections, 2018)

Adversarial Attacks können auch im Energiesektor auftreten, um gezielt KI-Algorithmen zu manipulieren. Besonders gefährdet sind Daten aus öffentlich zugänglichen Datenquellen. Hervorzuheben sind hier KI-basierte Prognosemodelle, die für ihre Prognosen auf öffentliche Satellitenbilder oder Wetterdaten zurückgreifen. Diese öffentlichen Daten bilden prinzipiell potenzielle Ziele für Hackerangriffe und könnten die Prognosen zu Gunsten des Hackers beeinflussen (auch wenn der Aufwand dafür enorm wäre). Neben externen Hackern besteht allerdings auch die Gefahr, dass Datenanbieter selbst ihre Daten vorsätzlich manipulieren, um eine profitable Verfälschung der Prognose zu erzielen.

> *KI-Methoden können so trainiert werden, dass sie fehlerhafte Daten oder feindliche Angriffe erkennen oder ihnen widerstehen können. Diese Maßnahmen sind jedoch nicht trivial in einer KI-Anwendung zu implementieren, daher muss diese Funktionalität neben dem primären Anwendungsfall selbst sorgfältig trainiert und bewertet werden.*

3.4 Zusammenfassung

Die Themen Datenerfassung, Datenquellen, Datenverfügbarkeit sowie Qualität bilden grundlegende Bereiche, denen für datengetriebene Anwendungen, insbesondere mit Fokus auf KI, eine besondere Bedeutung zukommen. Zusätzlich gehen mit diesen Themen Risiken und besondere Schutzanforderungen einher.

Eine automatisierte Datenerfassung und anschließende Archivierung bildet die Grundlage für jeden weiteren Schritt in Richtung Digitalisierung der eigenen betrieblichen Prozesse. Neben den Daten, die in den eigenen Händen liegen, bzw. im Unternehmen generiert oder erfasst werden

können, benötigen KI-Anwendungen oftmals zusätzliche Daten um einen Mehrwert für den jeweiligen Prozess zu generieren (z.B. verschneiden von Messzeitreihen mit Wetterdaten um Korrelationen zu identifizieren und zu nutzen). Hierzu sind neben den internen, eigenen Datenquellen, weitere zum Teil öffentliche Daten aber auch private Daten von Nutzen oder sogar notwendig. Hierzu wurde in Abschnitt 3.1.1 eine Auswahl dargestellt. Insgesamt ist, insbesondere die öffentliche, Datenlage noch nicht ausreichend und eine fehlende Open-Data Mentalität im Bereich der Energieversorgung lässt sich, zumindest aus wissenschaftlicher Sicht, feststellen. Es sei aber auch angemerkt, dass bestimmte strukturelle und personifizierte Daten unbedingt geschützt bleiben müssen.

Neben der Erfassung von Daten und deren Quellen, spielen die Verfügbarkeit und Qualität der Daten eine weitere wichtige Rolle. Nicht alle Informationen, die prinzipiell vorliegen können, können auch für die gewünschten Anwendungen genutzt werden. Da kann es bereits an nicht kompatiblen Formaten oder mangelnder Qualität scheitern. Eine Einordnung über die aktuelle Datenlage bei deutschen mittelgroßen bis kleinen VNB wurde in Kapitel 3.2 gegeben.

Abschließend wurde auf die durch die Nutzung von Daten entstehenden Risiken und möglichen Schutz eingegangen. Bei der Verwendung von datenbasierten Anwendungen ist man immer abhängig von der Richtigkeit der Daten (hier spielen auch Qualität und Verfügbarkeit eine grundlegende Rolle). Denn wenn bereits den Eingangsdaten nicht vertraut werden kann, wird das Ergebnis ebenfalls nicht belastbar sein (siehe hierzu auch Abschnitt 2.3.1). Aber auch schon allein das Sammeln und Halten der Daten stellen Risiken dar, bzgl. nicht autorisierten Zugriffen, bei denen Daten manipuliert oder entwendet werden können. Letzteres Risiko tritt insbesondere bei dem Transport bzw. der Übermittlung der Daten auf. Hier hilft nur ein verantwortungsbewusster Umgang mit den Daten und die Nutzung aktueller Verschlüsselungsverfahren und weiterer Schutzmaßnahmen.

4 Regulatorischer Rahmen

Durch die immer weiter ansteigende Nutzung von Daten für den Netzbetrieb, ist die Abhängigkeit von datengetriebenen Prozessen und Analysen stark angewachsen und kann, insbesondere bei Prozessen innerhalb kritischer Infrastrukturen, bei dem Ausfall der Prozesse oder einer Unterbrechung der Datenströme schnell problematisch werden. In Kapitel 2 wurden die Bereiche kritischer Prozesse sowie die Nutzung datengetriebener Anwendungen mit Fokus auf Anwendungen künstlicher Intelligenz näher beschrieben und auf potenzielle Risiken, aber auch neue Möglichkeiten, eingegangen. Auf die Daten an sich, bzgl. Beschaffung, Haltung, Kommunikation und Qualität, wurde in Kapitel 3 näher eingegangen. Hier wurde auch auf Probleme und Risiken aufmerksam gemacht, die mit der Nutzung von Daten und möglichen Abhängigkeiten im Netzbetrieb einhergehen.

Diese zunehmend vernetzten und datengetriebenen Prozesse in der Energiewirtschaft stellen neben neuen Anforderungen an den Betrieb des Stromnetzes auch Anforderungen an den regulatorischen Rahmen bzw. müssen bestehenden regulatorischen Anforderungen gerecht werden. Die mögliche Gefahr von Angriffen auf IT-Systeme fordert u.a. klar definierte Schutzziele und Maßnahmen, um einen Ausfall von relevanten Prozessen und Anwendungen in dieser kritischen Infrastruktur zu verhindern. Auch der Umgang mit Daten, speziell personenbezogenen Daten, erfordert Regelungen zum Schutz der betroffenen Unternehmen und Person vor kriminellem Missbrauch. Infolge der verstärkten Analyse und Nutzung von verschiedensten Arten von Daten und der ansteigenden Nutzung von Methoden der künstlichen Intelligenz im Bereich der Energieversorgung sowie in vielen Bereichen der Wirtschaft und Gesellschaft, besteht auch hier Bedarf an einem einheitlichen regulatorischen Rahmen für deren Verwendung und Einsatz.

In diesem Kapitel werden die relevantesten Gesetze zur Nutzung und Verarbeitung von Daten aufgezeigt sowie auf die daraus folgenden Anforderungen für den Umgang mit diesen Daten, im Kontext Datenschutz und -sicherheit, eingegangen und auch mögliche Hemmnisse aufgezeigt. Abschließend wird auf besondere Anforderungen bei der Verwendung von künstlicher Intelligenz hingewiesen und diese diskutiert.

4.1 Regulatorischer Rahmen für den Betrieb des Stromnetzes

Neben den Anforderungen, die sich aus der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz [21] ergeben (siehe Kapitel 2), werden weitere energiepolitische Rahmenbedingungen durch eine Vielzahl von Gesetzen und Verordnungen auf nationaler und internationaler Ebene vorgegeben. Regulatorische Rahmenbedingungen, die Einflüsse auf das Stromnetz haben, ergeben sich überwiegend aus den Bereichen Energierecht, IT-Sicherheit sowie Datenschutz und Datensicherheit. Die wichtigsten Grundsätze der Energiewirtschaft werden durch die Europäische Union (EU) geregelt. EU-Recht steht über nationalem Recht, weshalb alle Mitgliedsstaaten verpflichtet sind Richtlinien auf EU-Ebene in nationales Recht umzusetzen. Hierbei werden durch die EU Ziele vorgegeben, die innerhalb einer Frist erreicht werden müssen. Die Mittel, mit denen die Ziele erreicht werden, können dabei von den einzelnen Staaten frei gewählt werden. Verordnungen sind in allen EU-Mitgliedsstaaten rechtlich verbindlich und bedürfen nicht der

Umsetzung in nationales Recht. In Tabelle 4 sind die wichtigsten Gesetze im Überblick zu sehen, im Anschluss werden die Kernpunkte aus den Gesetzen und Verordnungen kurz erläutert, wobei auf das EnGW detaillierter eingegangen wird.

Energierecht & IT-Sicherheit	Datenschutz & Datensicherheit
Energiewirtschaftsgesetz (EnWG)	Datenschutzgrundverordnung (DSGVO)
Gesetz zur Digitalisierung der Energiewende (GDEW)	Bundesdatenschutzgesetz (BDSG)
Messstellenbetriebsgesetz (MsbG)	
IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)	
Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie)	

Tabelle 4: Übersicht der für den Betrieb des Stromnetzes relevanten Gesetze und Verordnungen.

Auf EU-Ebene wurde 2017 mit der Richtlinie zur **Netz- und Informationssicherheit (NIS-Richtlinie)** ein „einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cybersicherheit“ geschaffen. Hierin werden u.a. Mindestsicherheitsanforderungen wie Meldepflichten für kritische Infrastrukturen vorgegeben, die im IT-Sicherheitsgesetz 2.0 berücksichtigt worden sind. Außerdem wird der Rahmen für Anbieter von digitalen Diensten, wie z. B. Cloud-Services und Online-Marktplätzen, geschaffen. Seit Anfang 2022 wird über einen „neuen, harmonisierten europäischen Regulierungsrahmen für Cybersicherheit“ in Form einer NIS-Richtlinie 2.0 diskutiert [39].

Um der zunehmenden Bedrohung durch Cyber-Angriffe entgegenwirken zu können, wurde im April 2021 das **IT-Sicherheitsgesetz 2.0** verabschiedet, das für die IT-Sicherheit einen ganzheitlichen Ansatz beabsichtigt. Mit dem Gesetz werden Regelungen aus dem EnWG und verschiedenen anderen Gesetzen aufgegriffen und die Artikel aus den Stammgesetzen geändert. Thema ist u.a. die Detektion und Abwehr von Cyber-Angriffen mit dem Kernziel die Sicherheit informationstechnischer Systeme zu verbessern. Insbesondere an die Betreiber kritischer Infrastrukturen werden besondere Anforderungen gestellt, um die Cyber-Resilienz in kritischen Sektoren zu erhöhen [40].

Aus Sicht der Gesetzgebung nimmt neben dem Energiewirtschaftsgesetz und dem IT-Sicherheitsgesetz vor allem das **Gesetz zur Digitalisierung der Energiewende (GDEW)** Einfluss auf den Wandel des Energiesystems. Das GDEW wurde im April 2016 verabschiedet und befasst sich mit Themen wie der Ausstattung und dem Betrieb von intelligenten Messsystemen bei Erzeugern und Verbrauchern, wodurch der Aufbau einer digitalen Infrastruktur mit intelligenten Netzen ermöglicht wird [12].

Mit dem GDEW wurde das **Messstellenbetriebsgesetz (MSBG)** in der heutigen Fassung auf den Weg gebracht, mit dem der Einbau und Betrieb von modernen Messeinrichtungen und intelligenten Messsystemen geregelt wird. Bis 2032 müssen gemäß Messstellenbetriebsgesetz in allen Haushalten in Deutschland digitale Messeinrichtungen installiert werden. Das GDEW und MSBG

treffen zudem Regelungen zur Datenkommunikation mit Smart Meter Gateways sowie zur Erhebung, Verarbeitung und Nutzung von Daten unter der Berücksichtigung der Datensicherheit und des Datenschutzes.

EnWG

Eine zentrale Bedeutung für Betreiber von Energieversorgungsnetzen hat auf Bundesebene das **Energiewirtschaftsgesetz (EnWG)**. Im EnWG werden für alle Netzbetreiber allgemeine Vorgaben zum sicheren Betrieb von Energieversorgungsnetzen festgelegt. Der Betrieb soll so erfolgen, dass „eine sichere, preisgünstige, verbraucherfreundliche, effiziente und umweltverträgliche leitungsgebundene Versorgung mit Strom und Gas“ [12] gesichert ist. Konkrete Ziele sind u.a. die freie Preisbildung für Strom zu stärken und der Ausgleich von Angebot und Nachfrage auf Marktebene sowie der adäquate Einsatz von Stromerzeugungsanlagen, Stromverbrauchern und Speichern.

Auf der Grundlage des Energiewirtschaftsgesetzes (EnWG) wurde eine Reihe von Rechtsverordnungen erlassen, die in Tabelle 5 aufgeführt sind.

Verordnung
Elektrizitätssicherungsverordnung
Stromnetzzugangsverordnung
Stromnetzentgeltverordnung
Verordnung zu abschaltbaren Lasten
Netzreserveverordnung
Anreizregulierungsverordnung
Niederspannungsanschluss-Verordnung
Ladesäulenverordnung
Kraftwerks-Netzanschlussverordnung
Systemstabilitätsverordnung
Stromgrundversorgungsverordnung
Verordnung zum Schutz von Übertragungsnetzen

Tabelle 5: Verordnungen, die im Rahmen des Energiewirtschaftsgesetzes erlassen wurden.

Relevant im Zuge der Energiewende und Digitalisierung sind vor allem die Ladesäulenverordnung und die Anreizregulierungsverordnung.

Zur Erreichung der Klimaschutzziele ist der Ausbau der Elektromobilität im Verkehrssektor eine entscheidende Maßnahme. Ein wichtiger Bestandteil hierbei ist das Vorhandensein einer bedarfsgerechten Ladeinfrastruktur, sodass Nutzer von E-Kfz durch eine ausreichende Anzahl von Ladepunkten jederzeit und überall die Möglichkeit haben ihr Auto verlässlich zu laden [38]. Die Ladesäulenverordnung enthält technische Mindestanforderungen für den Aufbau und Betrieb von

öffentlich zugänglichen Ladesäulen sowie Anforderungen zum Aufladen an den Ladepunkten. Mit der am 1. Januar 2022 in Kraft getretenen Novelle der Ladesäulenverordnung sollen Ladevorgänge zukünftig weiter vereinfacht werden, indem die Zahlung auch mittels einer Debit- oder Kreditkarte möglich sein soll.

Die Verordnung über die Anreizregulierung (ARegV) legt den Rahmen für die Finanzierung und die Basis zur Ermittlung der Netzentgelte für die regulierten Netzbetreiber von Strom- und Gasnetzen fest. Darüber hinaus legt die Anreizregulierungsverordnung Vorgaben zur Effizienzsteigerung fest, die aus dem Effizienzvergleich der Netzbetreiber untereinander resultieren. Durch welche Maßnahmen die Effizienzvorgaben erfüllt werden, können Netzbetreiber innerhalb der Erlösobergrenze frei entscheiden.

> *Mit dem steigenden Anteil regenerativer Energieerzeugungsanlagen, die zu über 90 % im Verteilnetz angeschlossen werden, wächst auch der Bedarf an Investitionen in den Verteilnetzen, insbesondere an Maßnahmen zur Umsetzung der Digitalisierung, um durch effiziente Koordinierung den erzeugten Strom vollständig in das Netz einspeisen zu können. Da diese Ausgaben aber nicht als Investitionen (CAPEX), sondern als operative Kosten (OPEX) gewertet werden, werden diese u.U. nicht in die kalkulatorische Verzinsungsbasis gem. Anreizregulierungsverordnung einbezogen und stellen in der unternehmerischen Investitionsentscheidung eine unattraktivere Option dar. Das wiederrum motiviert nicht sonderlich in diese neuen Verfahren und Technologien zu investieren. Innovative, datengetriebene Anwendungen, die z.B. KI-Methoden nutzen, können aber einen großen Beitrag zur Optimierung des Netzes und der Effizienzsteigerung leisten und somit Betriebskosten senken. Da die Entwicklung und Einführung solcher Methoden meist mit Kosten verbunden sind, sollte diese auch von regulatorischer Seite aktiv animiert und unterstützt werden. Parallel dazu müssen die Auswirkungen auf die Netzentgelte im Interesse der Verbraucher berücksichtigt werden. [12]*

IKT-Sicherheit

Auch die IKT-Sicherheit wird im EnWG thematisiert. In §11 (1a) des EnWG wird gefordert, dass Netzbetreiber „einen angemessenen Schutz gegen Bedrohung für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind“ vorweisen müssen [24]. In diesem Rahmen wurde von der Bundesnetzagentur (BNetzA) gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ein IT-Sicherheitskatalog entworfen. Dieser fordert von allen Netzbetreibern, dass ein Informationssicherheits-Managementsystems (ISMS) installiert werden muss, das der international führenden Norm DIN EN ISO/IEC 27001 entspricht. Es geht dabei nicht um eine Beschreibung technischer Anforderungen, sondern um die Beschreibung eines Prozesses, bei dem das Gefährdungspotential abgeschätzt werden soll, um geeignete Gegenmaßnahmen ergreifen zu können. Strom- und Gasnetzbetreiber sind verpflichtet ein solches System zu nutzen und müssen sich entsprechend zertifizieren lassen. Das ist insbesondere vor dem Hintergrund von Prozessen in einer kritischen Infrastruktur hilfreich, die einzelnen Prozesse auf ihre potenziellen Schadensauswirkungen zu bewerten. Die dort verwendeten Indikatoren umfassen ähnliche Bereich wie die unter Kapitel 2.2 beschriebenen, sind aber allgemeiner formuliert.

Ergänzend wurden auf Basis der ISO/IEC 27000-Normenreihe weitere Standards definiert. Hierzu zählt u.a. ein Leitfaden (ISO/IEC 27002), der im Februar 2022 aktualisiert worden ist und der verschiedene Informationssicherheitsmaßnahmen detailliert erläutert ([21]). Zusätzlich enthält er Beispiele zur Anwendung, die in der Mehrheit von Unternehmen eingesetzt werden können. Im Gegensatz zu den Normen ISO/IEC 27001 und ISO/IEC 27002, die allgemein unabhängig von der konkreten Branche anzuwenden sind, ergänzt die ISO/IEC 27019 Einzelmaßnahmen und Maßnahmenziele in der Energieversorgungsindustrie. Insbesondere werden hier sektorspezifische Maßnahmen für die Bereiche Strom, Gas, Öl und Wärme beschrieben, die über die Maßnahmen der ISO/IEC 27001/2“ hinausgehen.

Die ISO/IEC 270xx-Verordnungen können in der Umsetzung als ISMS Gefahren und Risiken von Angriffen auf die eigene IT-Infrastruktur sowie Datenbestände reduzieren, indem sie Unternehmen dazu auffordern vorhandene und geplante IT-Prozesse detailliert zu beschreiben und potenzielle Gefahren und deren Auswirkungen auf das Unternehmen und deren Aufgaben abzuleiten, einzuordnen, zu bewerten und mögliche Gegenmaßnahmen zu entwickeln sowie diese umzusetzen. Allerdings erfordert eine konsequente ISMS Umsetzung personelle Ressourcen, die wiederrum zusätzliche Kosten verursachen und auch dazu führen können, dass innovative Anwendungen und Prozesse nicht eingeführt werden, weil der Aufwand an ISMS-Beschreibungen und möglichen Folgemaßnahmen zu hoch erscheint. Dieses kann zu einem Innovationsstau führen. Eine weitere Herausforderung auf dem Weg zur digitalen Transformation besteht aber gerade in der Modernisierung der IT-Systeme, die derzeit bei den meisten Unternehmen noch nicht ausreichend auf z.B. Cyber-Angriffe vorbereitet sind. Bestehende Systeme sind z.B. zum Teil veraltet und nicht mit den Anforderungen aktueller Sicherheitssysteme kompatibel.

4.1.1 Datenschutz

Im Gegensatz zur Datensicherheit (vgl. 3.3.2) befasst sich der Datenschutz nur mit personenbezogenen Daten, weshalb der Datenschutz einen Teilbereich der Datensicherheit bildet [12]. Der rechtliche Rahmen für personenbezogene Daten wird maßgeblich von der **Datenschutzgrundverordnung (DSGVO)** bestimmt und durch das Bundesdatenschutzgesetz (BDSG) ergänzt.

DSGVO – Datenschutz personenbezogene Daten

Gemäß der DSGVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Hierzu zählen u.a. biometrische Daten, Kundendaten oder IP-Adressen, sowie Sprach- und Videoaufzeichnungen von Personen. Durch die DSGVO soll jeder Person ein Recht auf informationelle Selbstbestimmung sowie der Schutz ihrer Daten vor missbräuchlicher Verwendung garantiert werden. Der Anwendungsbereich der DSGVO erstreckt sich nicht nur über alle Unternehmen, die ihren Sitz in der EU haben, sondern auch über Unternehmen außerhalb von Europa, sofern diese auf dem europäischen Markt agieren oder personenbezogene Daten von in der EU lebenden Bürgern verarbeiten.

Nach der DSGVO müssen verschiedene Grundsätze („Rechtmäßigkeit der Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht“) für die Verarbeitung personenbezogener Daten eingehalten werden. Die Weitergabe personenbezogener Daten wie auch die Speicherung

und Verarbeitung darf nur mit Zustimmung der betroffenen Person erfolgen. Darüber hinaus muss die Verarbeitung personenbezogener Daten immer zweckgebunden erfolgen und die Löschung erfolgen, sobald die Daten nicht mehr benötigt werden. Eine detaillierte Ausführung aller Grundsätze findet sich in der dena-Analyse „Datenschutz und Datensicherheit. Status quo, Herausforderungen und Handlungsbedarf im Rahmen der Digitalisierung der Energiewirtschaft [24]".

> *Die Zweckbindung kann in Verbindung mit der Datenerhebung von personenbezogenen Daten und deren Aufbewahrung für intelligente Anwendungen zu Schwierigkeiten führen, da z.B. bei KI-Anwendungen der finale Verwendungszweck häufig noch nicht eindeutig absehbar ist. Allerdings ist hier anzumerken, dass es aktuell in der wissenschaftlichen, anwendungsnahen Entwicklung im Bereich Netzbetrieb kein Ziel ist, Haushalte oder andere Entitäten detailliert zu analysieren oder zu prognostizieren. Vielmehr reichen für Anwendungen im Netzbetrieb anonymisierte und aggregierte personenbezogene Daten aus, die dann nicht mehr unter die Bedingungen der DSGVO fallen, um z.B. das Verbrauchsprofil einer Ladesäule oder eines Wohngebietes zu charakterisieren. Die DSGVO stellt somit auch kein signifikantes Hindernis in der Umsetzung und Anwendung datengetriebener oder KI-basierte Anwendungen dar. In der Use Case Übersicht in Tabelle 2 in Kapitel 2.3.2 benötigt keine der beschriebenen Anwendungen detaillierte personenbezogene Informationen.*

Auch an IT-Systeme und Prozesse werden durch die DSGVO konkrete Anforderungen gestellt, wobei die technologischen Schutzmaßnahmen dem Stand der Technik entsprechen müssen, um einen Missbrauch und unbefugten Zugriff auf Daten zu verhindern. Hierzu zählt beispielsweise die Verschlüsselung gespeicherter Daten. Technologische Schutzmaßnahmen sollen bereits im Entwicklungsprozess mit einbezogen werden, sodass technikbasierter Datenschutz („Privacy by design") von vorherein durch technische Möglichkeiten gesichert ist. Neben dem Grundsatz „Privacy by design" werden durch den Grundsatz „Privacy by default" datenschutzfreundliche Voreinstellungen gefordert, d.h. es soll durch Voreinstellungen gewährleistet sein, dass nicht mehr Daten verarbeitet werden als für den konkreten Vorgang notwendig sind.

> *Die Grundsätze „privacy by design" und „privacy by default" sind im Rahmen der Einführung neuer digitaler Geschäftsmodelle oder der Anwendungsentwicklung auf Basis innovativer Technologien relevant, bei denen es gilt die Regeln und Anforderungen der DSGVO bei der Umsetzung zu berücksichtigen und entsprechend der Verordnung anzupassen.*

Zur Nutzung von personenbezogen erfassten Daten muss zunächst eine Anonymisierung oder Pseudonymisierung erfolgen. Bei einer Anonymisierung wird der Personenbezug vollständig aufgehoben, sodass eine Re-Identifizierung ausgeschlossen ist. Dabei muss beachtet werden, dass neben eindeutigen Zuordnungen wie dem Namen oder der Adresse auch andere unscheinbare Informationen zu einer Identifizierung führen könnten. Sind Daten nicht direkt personenbezogen, könnten aber unter Hinzuziehen von weiteren Informationen Rückschlüsse auf die Identität geben, spricht man von pseudonymen Daten. Diese zusätzlichen Informationen, die eine Zuweisung ermöglichen könnten, müssen getrennt von den eigentlichen Daten aufgehoben werden. Eine Anonymisierung ist gegeben, wenn Daten beispielsweise aggregiert zur Verfügung gestellt werden. Dies ist im Bereich der Energienetze bei Smart Meter Daten der Fall. Mit Smart Metern werden u.a. personenbezogene Verbrauchs- und Erzeugungsdaten erhoben, gespeichert und verarbeitet, die Rückschlüsse über das Verhalten der in einem Haushalt lebenden Personen zulassen können und mit denen Nutzungsprofile einzelner Personen erstellt werden könnten.

> *Es existieren heute zahlreiche Verfahren, die mit anonymisierten Daten, z.B. durch Aggregation, hinreichend genaue Ergebnisse liefern, sodass die Verwendung von personenbezogenen Daten nicht notwendig ist. Neben der Datenaggregation existieren zudem weitere spezielle Verfahren zur Anonymisierung, um die Nutzung von sensiblen Daten zu ermöglichen, da anonymisierte Daten nicht mehr den Anforderungen der DSGVO unterliegen [24].*

4.2 Regulatorische Rahmenbedingungen für den Einsatz von KI

Methoden der künstlichen Intelligenz nehmen aufgrund ihrer Fähigkeiten einen besonderen Stellenwert ein, für die ergänzend zu dem reinen Umgang mit Daten eigenständige Regeln und Standards entwickelt werden. Aufgrund der zunehmen Popularität und dem vermehrten Einsatz von KI in fast allen Bereichen der Wirtschaft und Gesellschaft wurde von der Bundesregierung im Jahr 2018 eine „KI-Strategie“ veröffentlicht, die 2020 noch einmal aktualisiert wurde [43].

Die KI-Strategie der Bundesregierung soll dazu beitragen Normen und Standards im Bereich der künstlichen Intelligenz zu definieren, um Deutschland zu einem führenden KI-Standort zu machen. Als eines der zwölf Handlungsziele der KI-Strategie wurde im Herbst 2020 die „Deutsche Normungsroadmap Künstliche Intelligenz“ vorgestellt. Aktuell wird an einer Neuauflage der Normungsroadmap gearbeitet [43].

Normungsroadmap KI

Die Normungsroadmap-KI wurde von DIN und DKE erstellt, mit dem Ziel frühzeitig einen Handlungsrahmen zu schaffen, der die Wettbewerbsfähigkeit Deutschlands im Bereich der Künstlichen Intelligenz stärkt und „innovationsfreundliche Rahmenbedingungen für die Technologie der Zukunft schafft.“ Normen und Standards können dazu beitragen die Akzeptanz von KI-Systemen zu erhöhen, indem beispielsweise Regeln zur Beurteilung der Zuverlässigkeit der Resultate eines KI-Systems definiert werden. „Auch darüber hinaus gibt es noch viel Handlungsbedarf vor allem im Hinblick auf Sicherheit, Fairness, Robustheit, Transparenz und Angemessenheit der KI-Systeme und ihrer Entscheidungen. [43]“ Zur Erreichung der Ziele werden fünf Handlungsempfehlungen herausgegeben.

Die **erste Handlungsempfehlung** beschreibt die Umsetzung von Datenreferenzmodellen für die Interoperabilität von KI-Systemen. Hiermit soll die Zusammenarbeit unterschiedlicher Akteure und deren Systeme vereinfacht werden, z.B. mittels eines sicheren, zuverlässigen, flexiblen und zwischen den Technologien kompatiblen Datenaustauschs.

Die **zweite Handlungsempfehlung** umfasst die Erstellung einer KI-Basis-Sicherheitsnorm. Grundsätzlich gilt ein KI-System als IT-System, für dessen Sicherheit es bereits umfassende Anforderungen gibt, die in zahlreichen Normen und Standards aus verschiedenen Bereichen festgelegt sind. Um die Technologieentwicklung durch die komplexe und unübersichtliche Vielzahl an Vorschriften nicht zu erschweren oder sogar zu blockieren, wird eine allumfassende „KI-Umbrella-Norm“ als sinnvoll erachtet. Hierin sollen die vorhandenen Normen und Vorgaben für die IT-Sicherheit gebündelt und durch Aspekte, speziell die KI betreffend, ergänzt werden.

Die Ausgestaltung einer initialen Kritikalitätsprüfung von KI-Systemen ist die **dritte Handlungsempfehlung**. Eine risikoadaptive Beurteilung von Anwendungen soll, besonders in kritischen Bereichen, die Möglichkeit bieten die Kritikalität einer Anwendung einschätzen zu können. Für

bestimmte Anwendungsfelder könnten z.B. Qualitätsschranken definiert werden. Bei einer Unterschreitung ist eine Weiterverwendung der KI-Ergebnisse in einem kritischen Anwendungsbereich nicht zulässig. In den als unkritisch eingestuften Anwendungsfeldern hingegen soll die Möglichkeit der Entwicklung ohne besondere Anforderungen bestehen.

> *Ähnlich der Kritikalitätsbewertung anhand von Qualitätsschranken muss bereits jetzt eine Differenzierung bei dem Einsatz von Anwendungen im Stromnetz erfolgen. Hierbei muss geprüft werden welche Aufgabe die Anwendung übernimmt, d.h. greift sie beispielsweise in den direkten Betrieb des Stromnetzes ein oder gibt sie lediglich Handlungsempfehlen, deren Umsetzungsentscheidung aber weiterhin bei dem systemverantwortlichen Personal liegt. Zurzeit dienen die meisten Anwendungen nur zur Verbesserung von bestehenden Prozessen und unterstützen bei der Entscheidungsfindung, steuern aber nicht automatisiert den Netzbetrieb.*

In der **vierten Handlungsempfehlung** wird die Initiierung eines nationalen Umsetzungsprogramms 'Trusted AI' zur Stärkung der europäischen Qualitätsinfrastruktur beschrieben. Hierbei geht es um die Einführung verlässlicher Qualitätskriterien und Prüfverfahren zur Zertifizierung von KI-Systemen, mit denen beispielsweise Anforderungen an „die Verlässlichkeit, Robustheit, Leistungsfähigkeit und funktionale Sicherheit“ gestellt werden.

Die **fünfte Handlungsempfehlung** bezieht sich auf die Ableitung anwendungstypischer und branchenrelevanter Normungs- und Standardisierungsbedarfe für industriereife Anwendungen.

> *Die Details einer solchen Norm sind sehr anwendungsspezifisch, weshalb experimentelle Anwendungen im Stromnetz, die sich noch in der Forschungs- und Entwicklungsphase befinden, einen gewissen Reifegrad erreichen müssen, bevor Normen entwickelt werden können. Normungs- und Zertifizierungsverfahren sollten aber bereits in dieser Phase berücksichtigt werden, damit Testverfahren und Risikobewertungen gleichzeitig entwickelt und nahtlos in die KI-Lösung integriert werden können.*

Gesetz über Künstliche Intelligenz

Neben der deutschen Normungsroadmap-KI wurde im April 2021 erstmals ein „Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz)“ auf den Weg gebracht. Ziel ist es allgemeingültige Regeln im Zusammenhang mit KI-Anwendungen auf EU-Ebene für eine „KI made in Europe“ zu definieren. Kernpunkte des Gesetzes sind Sicherheitsaspekte wie eine Transparenzpflicht für bestimmte KI-Systeme sowie die Möglichkeit von Eingriffen in die Systeme als Sicherheitsmaßnahme, eine sogenannte „Stop Button“-Vorschrift. Darüber hinaus widmet sich ein Abschnitt dem Verbot bestimmter Praktiken im Bereich der künstlichen Intelligenz.

In dem Gesetzvorschlag wird zwischen unterschiedlichen Anwendungsbereichen und vier Risikoklassen differenziert, an die jeweils unterschiedliche Anforderungen gestellt werden. Social Scoring-Systeme zählen beispielsweise zu KI-Systemen, die den ethischen Grundsätzen in der EU widersprechen und von denen damit ein inakzeptables Risiko ausgeht, weshalb sie grundsätzlich verboten werden sollen. Auch als hochriskant eingestufte Anwendungen sollen strengen Anforderungen unterliegen. Hierzu gehören auch Systeme zur Verwaltung und zum Betrieb kritischer Infrastrukturen, worunter das Stromnetz fällt, da ein Ausfall oder eine Störung das Leben und die Gesundheit von Menschen gefährden können.

> *Hierbei muss allerdings wieder differenziert werden, welche Aufgabe eine KI-Anwendung tatsächlich hat. Meist dienen die Anwendungen derzeit nur zur Verbesserung von bestehenden Prozessen und unterstützen bei der Entscheidungsfindung, übernehmen aber keine automatisierte Verantwortung für den Netzbetrieb.*

4.3 Zusammenfassung

Zusammenfassend lässt sich sagen, dass die aktuellen gesetzlichen und regulatorischen Rahmenbedingungen keine unüberwindbaren Hürden für den Einsatz datengetriebener Prozesse und KI-Anwendungen darstellen. Die Beachtung der sich daraus ergebenden Anforderungen fördert den sicheren Netzbetrieb, stellen aber durchaus einen z.T. beachtlichen Aufwand dar. Dieser kann dazu führen, dass innovative Umstellungen von betriebsinternen Prozessen oder die Einführung neuer Prozesse und Anwendungen aufgeschoben oder nicht durchgeführt werden. Hier sei als Beispiel der Aufwand zur Beschreibung der Prozesse innerhalb des ISMS nach ISO27001-Verordnung genannt.

Spezielle Verordnungen zum Schutz personifizierter Daten, wie die DSGVO, stellen zwar z.T. drastische Einschränkungen in der Verwendung von (personifizierten) Daten dar, die aber durch Pseudonymisierung und Anonymisierung, zumindest im Bereich des Netzbetriebs, bewältigt werden können. In den Anwendungen der Tabelle 2 werden z.B. keine detaillierten personifizierten Daten benötigt.

Im Bereich der KI-Anwendungen stellt die KI-Strategie der Bundesregierung einen signifikanten ersten Schritt in die Standardisierung und Normierung dieser Art von Anwendungen dar. Sie definiert z.B. in der Normungsroadmap-KI verschiedene Handlungsempfehlungen im Umgang mit der Datengrundlage aber auch in der Bewertung der Ergebnisse von KI-Anwendungen. Weiterhin werden u.a. die Entwicklung einer Sicherheitsnorm und Qualitätskriterien empfohlen, was hier als sehr sinnvoll erachtet wird. In dem *Gesetz über künstliche Intelligenz* werden u.a. auch ethische Aspekte adressiert. Diese sind allerdings bei den heutigen und in naher Zukunft absehbaren KI-Anwendungen im Stromnetz nicht sonderlich relevant.

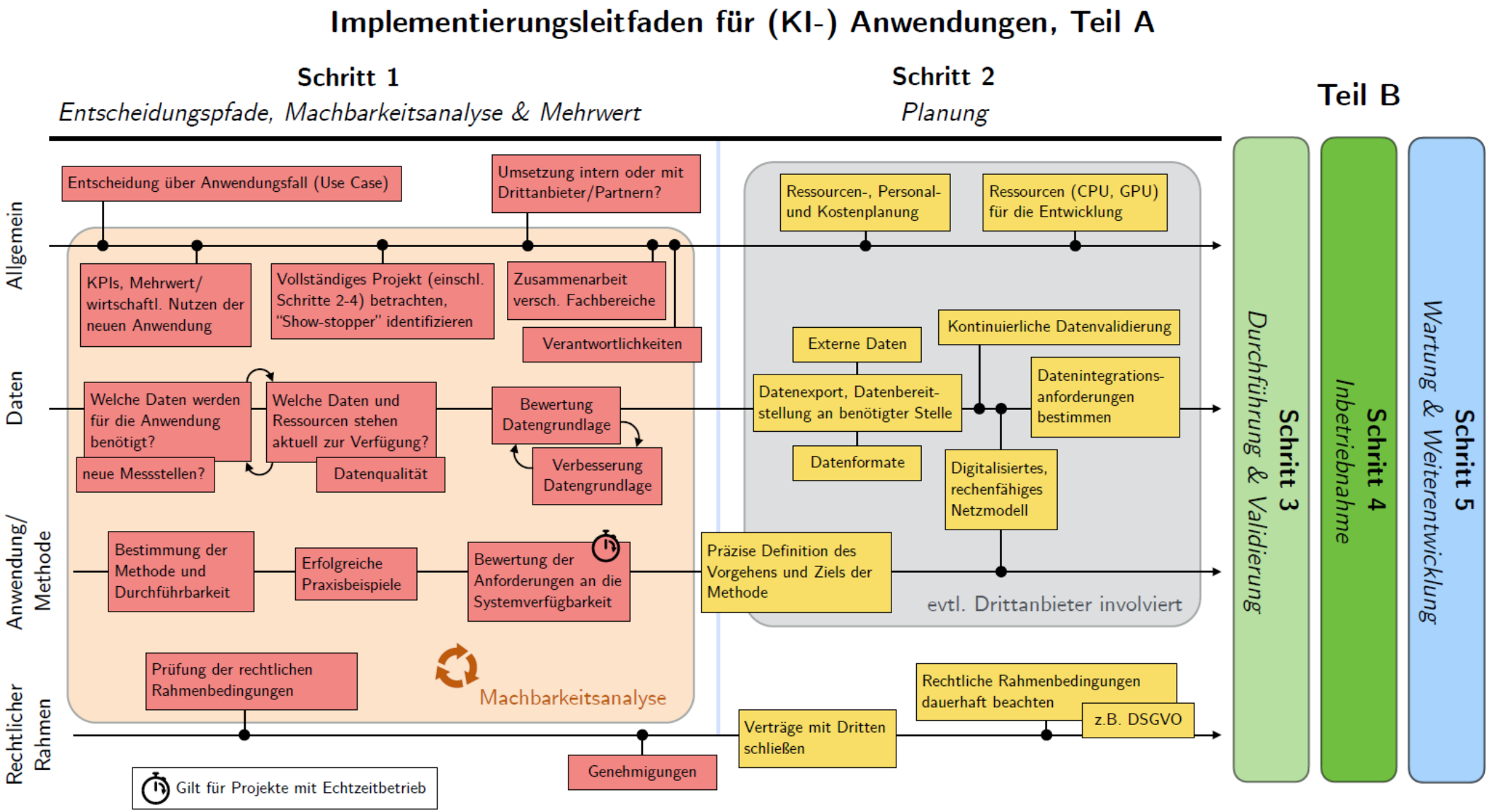
5 Implementierungsleitfaden

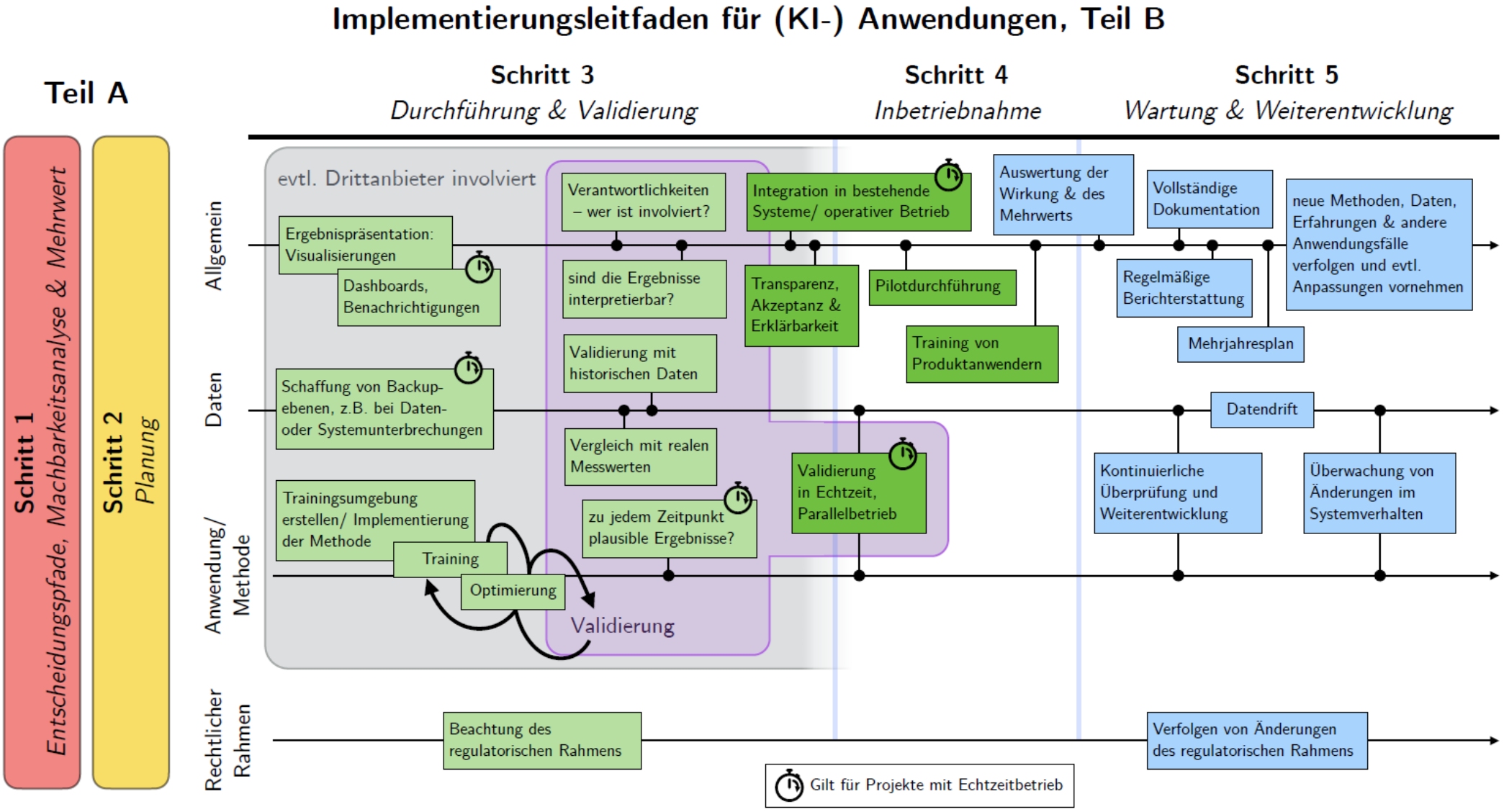
Datenanalysen bis hin zu KI-Anwendungen spielen zunehmend auch im Stromverteilernetz eine bedeutendere Rolle. Der Bedarf an neuen Entwicklungen, die auf intelligenten Methoden aufbauen, ist groß, beispielsweise im Bereich der E-Mobilität oder im Rahmen von Smart Homes. Einige große Verteilnetzbetreiber haben bereits eigene Entwicklungsabteilungen aufgebaut, um an der Umsetzung von intelligenten Datenanalysemethoden zu arbeiten. Vor allem für kleinere Netzbetreiber gestaltet sich die Einführung solcher Anwendungen aber schwierig. Während der Netzbetreiber-Workshops, die im Rahmen der Gutachtenerstellung durchgeführt wurden, kristallisierte sich der Wunsch vieler Netzbetreiber nach einem Leitfaden für die Einführung von innovativen Anwendungen heraus. Als ein primäres Hindernis bei der Einführung von intelligenten Anwendungen wurde u.a. fehlendes Know-How genannt, sowohl in Bezug auf die Möglichkeiten von intelligenten Methoden selber als auch auf das Vorgehen, z.B. welche Aspekte bei der Einführung zu beachten sind. Um diese Hürde zu reduzieren und die Einführung von innovativen Anwendungen für Netzbetreiber zu erleichtern, wurde ergänzend zu den beschriebenen Kernelementen des wissenschaftlichen Gutachtens ein Implementierungsleitfaden entwickelt. Dieser soll als grundlegende Orientierung dienen und die wesentlichen Schritte und Überlegungen abbilden, die über die verschiedenen Phasen einer Einführung von Datenanalysen im Unternehmen relevant sind. Zwei Fragen sollen damit adressiert werden:

1. *Was muss in der Planungs- und Vorbereitungsphase beachtet werden und welche Informationen sind hier relevant?*
2. *Wie kann die Durchführung aber auch nachhaltige Verwendung sichergestellt werden?*

Der Leitfaden gliedert sich daher in zwei Teile. Teil A beschreibt die ersten Schritte der Entscheidungsfindung mit dem Fokus auf die Datengrundlage sowie die Planung der Umsetzung und Durchführung. In Teil B wird die Umsetzung der Anwendung selbst behandelt sowie der Betrieb und eine nachhaltige Weiterentwicklung. Beide Teile des Leitfadens sind identisch aufgebaut und besitzen jeweils einen Zeitstrahl mit den Themenfeldern „Allgemein“, „Daten“, „Methode/ Anwendung“ und „Regulatorischer Rahmen“. Überschneidungen zwischen den Feldern sind möglich. Bestimmte Schritte sind nur für Echtzeitanwendungen relevant, wie z.B. Netzzustandsschätzungen in Echtzeit, im Gegensatz zu Netzplanungsprojekten. Diese Boxen sind mit dem Symbol einer Uhr gekennzeichnet.

In Kapitel 5.1 werden die einzelnen Aspekte der jeweiligen Schritte u.a. anhand von definierten Leitfragen noch einmal detaillierter vorgestellt. Hierbei werden relevante Fragestellungen aufgegriffen, die vor dem Einsatz und während der Planung einer solchen Anwendung beantwortet werden sollten. Der Leitfaden ist zur Orientierung gedacht und gilt nicht als verbindliche Umsetzungsvorschrift. Je nach gewählter Art des Projektes, ist es z.B. ein Forschungsprojekt, handelt es sich um eine Piloteinführung oder soll eine bereits etablierte Anwendung eingeführt werden, sind weitere Differenzierungen des Leitfadens nötig, u.a. in Bezug auf die Verfügbarkeiten oder Grenzen der Systeme, die in zukünftigen Projekten ausgearbeitet werden könnten. In Kapitel 5.2 wird der Implementierungsleitfaden beispielhaft für drei ausgewählte Anwendungsfälle durchlaufen, um die Aspekte des Leitfadens anschaulich z.B. mit konkreten Angaben zu den Datenanforderungen darzustellen.


Implementierungsleitfaden für (KI-) Anwendungen, Teil A
Schritt 1
Entscheidungspfade, Machbarkeitsanalyse & Mehrwert
Schritt 2
Planung
Teil B
Allgemein
Daten
Anwendung/ Methode
Rechtlicher Rahmen
Entscheidung über Anwendungsfall (Use Case)
Umsetzung intern oder mit Drittanbieter/Partnern?
KPIs, Mehrwert/ wirtschaftl. Nutzen der neuen Anwendung
Vollständiges Projekt (einschl. Schritte 2-4) betrachten, "Show-stopper" identifizieren
Zusammenarbeit versch. Fachbereiche
Verantwortlichkeiten
Welche Daten werden für die Anwendung benötigt?
neue Messstellen?
Welche Daten und Ressourcen stehen aktuell zur Verfügung?
Datenqualität
Bewertung Datengrundlage
Verbesserung Datengrundlage
Bestimmung der Methode und Durchführbarkeit
Erfolgreiche Praxisbeispiele
Bewertung der Anforderungen an die Systemverfügbarkeit
Prüfung der rechtlichen Rahmenbedingungen
Machbarkeitsanalyse
Ressourcen-, Personal- und Kostenplanung
Ressourcen (CPU, GPU) für die Entwicklung
Externe Daten
Kontinuierliche Datenvalidierung
Datenexport, Datenbereit-stellung an benötigter Stelle
Datenintegrations-anforderungen bestimmen
Datenformate
Digitalisiertes, rechenfähiges Netzmodell
Präzise Definition des Vorgehens und Ziels der Methode
evtl. Drittanbieter involviert
Rechtliche Rahmenbedingungen dauerhaft beachten
z.B. DSGVO
Verträge mit Dritten schließen
Genehmigungen
Gilt für Projekte mit Echtzeitbetrieb
Schritt 3
Durchführung & Validierung
Schritt 4
Inbetriebnahme
Schritt 5
Wartung & Weiterentwicklung


Implementierungsleitfaden für (KI-) Anwendungen, Teil B
Teil A
Schritt 1
Entscheidungspfade, Machbarkeitsanalyse & Mehrwert
Schritt 2
Planung
Schritt 3
Durchführung & Validierung
Schritt 4
Inbetriebnahme
Schritt 5
Wartung & Weiterentwicklung
Allgemein
Daten
Anwendung/ Methode
Rechtlicher Rahmen
evtl. Drittanbieter involviert
Ergebnispräsentation: Visualisierungen
Dashboards, Benachrichtigungen
Verantwortlichkeiten – wer ist involviert?
Integration in bestehende Systeme/ operativer Betrieb
Auswertung der Wirkung & des Mehrwerts
Vollständige Dokumentation
neue Methoden, Daten, Erfahrungen & andere Anwendungsfälle verfolgen und evtl. Anpassungen vornehmen
sind die Ergebnisse interpretierbar?
Transparenz, Akzeptanz & Erklärbarkeit
Pilotdurchführung
Regelmäßige Berichterstattung
Training von Produktanwendern
Mehrjahresplan
Schaffung von Backup-ebenen, z.B. bei Daten- oder Systemunterbrechungen
Validierung mit historischen Daten
Datendrift
Vergleich mit realen Messwerten
Validierung in Echtzeit, Parallelbetrieb
Kontinuierliche Überprüfung und Weiterentwicklung
Überwachung von Änderungen im Systemverhalten
Trainingsumgebung erstellen/ Implementierung der Methode
Training
Optimierung
zu jedem Zeitpunkt plausible Ergebnisse?
Validierung
Beachtung des regulatorischen Rahmens
Verfolgen von Änderungen des regulatorischen Rahmens
Gilt für Projekte mit Echtzeitbetrieb

5.1 Leitfaden für den Einsatz von innovativen, datengetriebenen Anwendungen im Stromnetz

In diesem Kapitel werden die einzelnen Schritte des Leitfadens, u.a. durch aufgestellte Leitfragen zu den einzelnen Punkten, die im Rahmen der Umsetzung als Orientierung dienen können, detaillierter aufgegriffen.

> *Schon zu Beginn sollten alle Schritte des Leifadens Schritt für Schritt durchgespielt und durchdacht werden, um bereits im Vorfeld mögliche „Showstopper" zu identifizieren und an kritischen Stellen Abbruchkriterien zu definieren.*

Schritt 1: Entscheidungspfade, Machbarkeitsanalyse und Mehrwert

Entscheidung über den Anwendungsfall (Use Case)

An erster Stelle steht bei Schritt 1 die Auswahl des Anwendungsfalls. Eine Übersicht über eine Auswahl an möglichen Anwendungsfällen findet sich unter Kapitel 2 in Tabelle 2. Ein wichtiges Entscheidungskriterium kann eine Machbarkeitsanalyse darstellen. In der folgenden Tabelle werden u.a. mögliche Aspekte und Leitfragen vorgestellt, die bei der Entscheidungsfindung unterstützen können.

Allgemein	**Mehrwert der Anwendung** - Welchen Mehrwert, insbesondere wirtschaftlichen Nutzen, liefert die Anwendung? - Welche KPIs lassen sich definieren?
	Definition von Verantwortlichkeiten im Unternehmen - Wer ist im Unternehmen involviert und bei wem liegen die Verantwortlichkeiten (Product Owner, Projektleiter, etc.)? ➢ *Für die erfolgreiche Umsetzung ist eine Zusammenarbeit von mehreren Fachbereichen notwendig (Asset Management, Netzplanung, IT, Techniker, etc.)!*
	Bestimmung der Umsetzungsart - Soll die Umsetzung intern (eigene Entwicklung) oder durch Drittanbieter/ mit Partnern (Nutzung bereits vorhandener Entwicklungen sowie Expertenwissen) erfolgen? - Kann KI aus Forschungsvorhaben mit ähnlichen Zielen verwendet werden?
Daten	**Bewertung der zur Verfügung stehenden Daten und Ressourcen** - Welche Daten werden aktuell gespeichert und aus welchem System kommen welche Informationen? - Wie ist die vorhandene Datengrundlage sowohl qualitativ als auch quantitativ zu bewerten? - Ist die zeitliche Auflösung der Daten und ist das Zugriffsintervall von Messdaten ausreichend? - Kann oder muss die Datengrundlage verbessert werden?

Daten	**Anforderungen an die Datenerfassung** - Welche Datenarten werden für die Anwendung benötigt (Kundendaten, Anlagendaten, externe Daten, …)? - Müssen neue Messstellen oder Sensorik eingerichtet werden? - Erfordert der beabsichtigte Use Case eine Datenerfassung in Echtzeit?
Anwendung/ Methode	**Bewertung der Anforderungen an die Systemverfügbarkeit** - Welche Auswirkungen hat eine Systemunterbrechung? - Würde eine kritische Situation entstehen, wenn das System offline gehen würde? **Bestimmung der Methode und ihrer Durchführbarkeit** - Wie ist der Entwicklungsstand zu dem Use Case? - Gibt es bereits erfolgreiche Praxisbeispiele?

Regulatorischer Rahmen	**Prüfung der rechtlichen Rahmenbedingungen**
	- Welche rechtlichen Rahmenbedingungen muss man in diesem Anwendungsfall beachten?
	- Kann man vorhandene Daten uneingeschränkt nutzen?
	  ➢ Werden personenbezogene Daten genutzt? Müssen Daten anonymisiert werden?
	  ▪ Beachtung der DSGVO
	- Müssen Genehmigungen eingeholt werden?
	- Müssen besondere Regelungen bei der Nutzung von KI beachtet werden?

Tabelle 6: Schritt 1 des Implementierungsleitfadens.

Nach Schritt 1 sollte die Entscheidung über den Anwendungsfall gefallen sein und dessen Mehrwert für das Unternehmen feststehen. Auch die Durchführbarkeit des Projekts sollte bestätigt und eine erste Projektskizze erstellt werden. Dafür sollten Kenntnisse über die Datengrundlage vorhanden sein, z.B. welche Daten aus welchem System kommen und aktuell zur Verfügung stehen. Ebenso sollten wichtige Verantwortungsfragen, wer welche Rolle übernimmt, innerhalb des Unternehmens beantwortet sein. Insbesondere sollten Fragen zum Datenbedarf und deren Verfügbarkeit mit den jeweils relevanten Personen geklärt worden sein. Auch die relevanten rechtlichen Aspekte sollten nach dieser Phase evaluiert und berücksichtigt worden sein. Gerade für den Fall, dass es intern noch keine weitreichende Erfahrung mit diesen Themen gibt, empfiehlt es sich externe Expertise hinzuzuziehen.

Schritt 2: Planung

In Schritt 2 soll eine ausführliche Planung zur Umsetzung der ausgewählten Anwendung erfolgen. Hierzu zählen die Ressourcen, Personal- und Kostenplanung sowie eine präzise Definition des Vorgehens und des Ziels der Anwendung. Auch die konkreten Anforderungen an die benötigten Daten müssen festgelegt werden.

Allgemein	**Ressourcen-, Personal- und Kostenplanung** - Wie viel Personal wird für die Umsetzung der Anwendung benötigt? - Welche Kosten müssen für das Personal während der Entwicklung, Inbetriebnahme und Wartung kalkuliert werden? - Entstehen Kosten durch Drittanbieter? Wenn ja wie hoch und gibt es Folgekosten? - Welche Ressourcen werden für das Auf- und Umsetzen der Methoden und Anwendungen benötigt (Hardware/ Software/ Lizenzen, …)? In welcher Form werden diese benötigt? - Entstehen Kosten durch die Nutzung externer Daten, z. B. Wetterdaten? Und wenn ja, fallen mögliche Folgekosten an? - Entstehen Kosten für zusätzlich benötigte Infrastruktur, Software, Cloud-Computing, Server, etc.? Und wenn ja, fallen mögliche Folgekosten an?

Daten	**Präzise Festlegung der konkreten Datenanforderungen**
	Eine kontinuierliche Datenvalidierung ist unerlässlich, um die Daten erfolgreich nutzen zu können.
	- Welche Daten werden benötigt?
	  ➢ In welchem Format werden die Daten jeweils benötigt?
	  ➢ Über welchen Zeitraum werden welche Daten benötigt (z.B. jahreszeitabhängig)?
	  ➢ Müssen zur Aufnahme benötigter Daten neue Messstellen eingerichtet werden?
	- Wie ist die Datenqualität?
	  ➢ Gibt es Lücken in den Daten? Wie können diese gefüllt werden?
	- Liegt ein digitalisiertes, rechenfähiges Netzmodell vor, z.B. in Siemens PSS Sincal, CIM, DIgSILEND PowerFactory, NEPLAN, etc.?

	Prüfung der Möglichkeiten zur Datenbereitstellung an benötigter Stelle - Können die Daten aus den vorhandenen Systemen exportiert werden? - Gibt es einen zentralen Speicherort für alle Daten? ➢ Nutzung von Datenbanken, Cloudspeichern, etc.? - Gibt es eine Anbindungsumgebung, in der die Daten zusammengefügt werden können?

Anwendung/ Methode	**Präzise Definition des Vorgehens und des Ziels der Methode** - Welche Meilensteine und Ziele sollen definiert werden? - Erstellung einer präzisen Beschreibung der zu verwendenden Methode ➢ Ist die Methode z.B. eine komplette Blackbox oder kann sie Zwischen- oder Modulergebnisse liefern, die überprüfbar sind?

Regulatorischer Rahmen	**Erstellung von Verträgen, detaillierte Prüfung der Rechtsabteilung**
	- Müssen Verträge mit Dritten geschlossen werden? (Sollten Partner oder Drittanbieter involviert sein)
	  ➢ Gibt es z.B. Geheimhaltungsverpflichtungen?
	- Sind alle ISMS Maßnahmen erfüllt?
	  ➢ Müssen evtl. externe Dienstleister eine Selbstauskunft ausfüllen?
	  ➢ Gibt es technisch organisatorische Maßnahmen (TOMs) zu beachten?
	- Sind alle Daten, die benutzt werden müssen, auch frei zur Weitergabe an externe Dienstleister? (z.B. Prognosen eines externen Anbieters)

Tabelle 7: Schritt 2 des Implementierungsleitfadens.

Spätestens nach Schritt 2 sollten die konkreten Datenanforderungen feststehen, die für die Umsetzung der Anwendung essenziell sind und an geeigneter Stelle bereitgestellt werden können. Für viele Anwendungen ist ein rechenfähiges Netzmodell erforderlich, das nach diesem Schritt ebenfalls vorliegen sollte. Auch der Rahmen für die Kosten des Personals und der benötigten Ressourcen sollte abgegrenzt worden sein. Der Projektablauf sollte detailliert beschrieben sein, um das Vorgehen erfolgreich zu starten. Hinzu kommt die Vorabklärung des rechtlichen Rahmens. Hier ist insbesondere sicherzustellen, dass die zu verwendenden Daten frei sind von Rechten Dritter und auch keine personalisierten Informationen enthalten. Außerdem muss der Umgang der Daten mit potenziellen externen Dienstleistern geklärt werden, sowie die Integration und Beschreibung der neuen Prozesse in das eigene ISMS geklärt und sichergestellt werden.

Schritt 3: Durchführung & Validierung

Schritt 3 widmet sich der Durchführung bzw. Implementierung der Anwendung und der Validierung der Ergebnisse, die einen besonders wichtigen Punkt in dieser Phase ausmacht. Neben der Entwicklung der Anwendung sollte bereits an die Ergebnisdarstellung gedacht werden, um die Ergebnisse dem jeweiligen Anwender in geeigneter Form zu präsentieren. Hierbei sollten relevante Informationen herausgestellt werden, um den Entscheidungsprozess, z.B. für das Personal einer Leitwarte, zu vereinfachen.

Allgemein	**Validierung der Ergebnisse**
	- Wer ist für die Ergebnisvalidierung zuständig/ geeignet?
	  ➢ Können die Entwickler die Ergebnisse selber deuten und validieren?
	  ➢ Kann internes Personal die Ergebnisse interpretieren und validieren?

	Ergebnisdarstellung - Sind Visualisierungen (z.B. Dashboards) sinnvoll? Wenn ja, in welcher Form? - Können automatisierte Benachrichtigungen einen Mehrwert bieten (z.B. per Mail oder SMS, wenn die Anwendung einen kritischen Zustand erkennt)? ➢ im Echtzeitbetrieb empfehlenswert
Daten & Anwendung/ Methode	**Entwicklung, Training & Optimierung** - Was wird zur Implementierung der Methode benötigt? - Ist die Erstellung einer Trainingsumgebung notwendig? - Treten in der Trainings- und Entwicklungsphase inklusive Optimierung Fehler auf, die noch behoben werden müssen? - Müssen Backup-Ebenen, z.B. bei Daten- oder Systemunterbrechungen, geschaffen werden?

	Validierung
	- Welche Validierung kommt für die Anwendung in Frage?
	  ➢ Validierung anhand von realen (historischen) Messungen?
	  ➢ Validierung in Echtzeit (z.B. Parallelbetrieb)?
	- Sind die Ergebnisse zu allen Zeitpunkten plausibel und interpretierbar?
	- Ist die erzielte Ergebnisgüte höher als bei alternativen Methoden/Ansätzen?

Regulat. Rahmen	**Beachtung des regulatorischen Rahmens** - Sind während der Umsetzungsphase bestimmte Regelungen zu beachten (z.B. bei dem Einsatz von KI-Methoden)?

Tabelle 8: Schritt 3 des Implementierungsleitfadens.

In Schritt 3 erfolgt nach der Entwicklungsphase die erste (prototypische) Implementierung der Anwendung. Um zu prüfen, ob die entwickelte Anwendung fehlerfrei läuft und plausible Ergebnisse liefert, ist eine Validierungsphase unerlässlich. In den meisten Fällen entsteht eine sich wiederholende Schleife zwischen Validierung und Optimierung der Anwendung, wobei in der Optimierungsphase identifizierte Fehler korrigiert werden. Wenn die Prozesse aus Schritt 3 erfolgreich durchgeführt wurden, steht am Ende eine erfolgreich validierte Anwendung, deren Ergebnisse für die späteren Nutzer so dargestellt werden können, dass sie einfach zu verstehen sind und der Mehrwert der Anwendung erkennbar ist.

Schritt 4: Inbetriebnahme

In Schritt 4 erfolgt die Inbetriebnahme der entwickelten Anwendung. Hierzu gehört die Integration in die bestehenden Systeme sowie die Einführung innerhalb der betroffenen Bereiche des Unternehmens, z.B. beim operativen oder planerischen Personal. Um einen wirklichen Erfolg zu verzeichnen, ist es essentiell, dass die Anwendung innerhalb des Unternehmens auf Akzeptanz stößt. Eine frühzeitige Erkennbarkeit des Mehrwerts kann die Bereitschaft zur Anwendung neuer Methoden steigern. Beim Personal, dass die Methodik anwenden soll, muss sich der Mehrwert durch die Nutzung ergeben, sodass auch ein Mehrwert für das Unternehmen generiert wird.

Allgemein	**Integration in bestehende Systeme und den operativen Betrieb**
	- Wie lässt sich die Anwendung am besten integrieren?
	  ➢ Vor allem Anwendungen, die extern entwickelt wurden, stellen oftmals zusätzliche Herausforderungen an die Systemintegration
	Transparenz & Akzeptanz im Unternehmen schaffen
	Erfolgserlebnisse sind ein wichtiger Faktor!
	- Sind die Ergebnisse der entwickelten Anwendung für den Anwender leicht verständlich und einfach zu nutzen?
	  ➢ Visualisierung relevanter Ergebnisse beispielsweise via Dashboards
	  ➢ Benachrichtigungen beispielsweise mit Handlungsempfehlungen
	- Ist eine Schulung von Nutzern sinnvoll, damit alle entwickelten Funktionalitäten bekannt sind und eingesetzt werden können?
	- Kann eine demonstrative Pilotdurchführung zur Sichtbarkeit und dem Erfolg beitragen?

Daten & Anwendung/ Methode	**Einführung der Anwendung** - Ist ein Parallelbetrieb möglich und sinnvoll, um Vertrauen aufzubauen? - Lassen sich die Eingangs- und Ausgangsdaten im Echtzeitbetrieb bereitstellen und verwerten? - Gibt es Performanceprobleme aufgrund zu hoher Auslastung der Hardware? - Gibt es Rückfallprozesse im Falle von Datenausfällen, -fehlern oder Systemabstürzen?
Regulat. Rahmen	**Beachtung des regulatorischen Rahmens** - Sind während der Inbetriebnahme bestimmte Regelungen zu beachten (z.B. bei dem Einsatz von KI-Methoden)?

Tabelle 9: Schritt 4 des Implementierungsleitfadens.

Nach Schritt 4 ist das Ziel größtenteils erreicht! Eine funktionierende Anwendung ist entwickelt und konnte in die bestehenden Systeme integriert werden. Durch geeignete Maßnahmen, wie z.B. einen Parallelbetrieb zu vorhandenen Anwendungen, kann das Vertrauen in die Ergebnisse der Anwendung gestärkt werden. Besonders im Bereich von kritischen Prozessen (siehe Kapitel 2) ist zunächst ein Parallelbetrieb empfehlenswert, um die Ergebnisse der Anwendung über einen längeren Zeitraum überprüfen zu können und eine Vertrauensbasis in die Anwendung und deren Ergebnisse aufzubauen Schulungen für das Personal können ebenfalls dazu beitragen, dass alle Funktionalitäten der neuen Anwendung bekannt sind und eingesetzt werden können, um Prozesse zu verbessern oder bei Entscheidungen zu unterstützen.

Schritt 5: Wartung & Weiterentwicklung

Schritt 5 ist der letzte Schritt des Leitfadens, jedoch sollte ab hier eine kontinuierliche Wartung und Weiterentwicklung stattfinden.

Allgemein	**Vollständige Dokumentation während des gesamten Projekts** *Eine vollständige Dokumentation während des gesamten Projekts ist unerlässlich, falls später Anpassungen notwendig sind und z.B. die Personen, die die Anwendung entwickelt haben, nicht mehr im Unternehmen tätig sind!*
	Auswertung der Wirkung und des Mehrwerts der Anwendung - Wurden die zu Beginn definierten Ziele erreicht?
	Regelmäßige Berichterstattung - Können Mehrjahrespläne (z.B. 5-Jahres-Plan, etc.) definiert werden?
	Kontinuierliche Überprüfung und Weiterentwicklung - Gibt es neue Methoden, Erfahrungen oder andere Anwendungsfälle, die miteinbezogen werden können und evtl. Anpassungen nötig machen? - Überwachung von Änderungen im Systemverhalten - Wie kann das Verfahren weiterhin robust gegenüber häufigen Fehlern gemacht werden?
Daten & Anwendung/ Methode	**Kontinuierliche Überwachung der Daten** - Ist die Sicherung der Datenqualität gewahrt? - Können die Daten auch weiterhin zur Verfügung gestellt werden? Sind Änderungen z.B. in den Datenmodellen zu erwarten? - Gibt es vielleicht mittlerweile besser geeignete Datenquellen, die zukünftig (mit) verwendet werden sollten?

Daten & Anwendung/ Methode	**Datendrift identifizieren und reagieren**
	- Werden Methoden genutzt, die Anpassungen erfordern?
	  ➢ bei NN z.B. müssen die Netze nachtrainiert werden
	- Gibt es Änderungen in der Netztopologie?
	  ➢ Netzmodelle müssen aktuell gehalten werden
	- Gibt es Änderungen in verwendeten repräsentativen Daten?
	  ➢ Standardlastprofile verändern sich

Regulat. Rahmen	**Gibt es Änderungen des regulatorischen Rahmens, die Einfluss auf die Anwendung nehmen?** - Wurden z.B. neue Regelungen zum Einsatz von KI getroffen, die beachtet werden müssen?

Tabelle 10: Schritt 5 des Implementierungsleitfadens.

5.2 Implementierungsleitfaden für drei ausgewählte Use Cases

In diesem Kapitel wird der Implementierungsleitfaden beispielhaft für drei konkrete Use Cases durchlaufen. Hierbei werden die oben beschriebenen grundlegenden Aspekte der Schritte 1 bis 5 des Leitfadens behandelt, individuelle Anpassungen je nach Methode und Unternehmen werden aber notwendig sein und können nicht immer mit einbezogen werden.

Die hier dargestellten Anwendungsfälle wurden unter verschiedenen Kriterien ausgewählt. Ein Kriterium für die Auswahl war die aktuelle und zukünftige Relevanz des Anwendungsfalls für die Verteilnetzbetreiber. Hierzu wurden innerhalb der im Gutachten durchgeführten Netzbetreiberworkshops Umfragen durchgeführt, worin mehrheitlich die fehlende Netztransparenz in der Mittelspannung als Herausforderung identifiziert wurde. Um der Forderung nach mehr Sichtbarkeit zu begegnen, steht als Use Case die MS-Netzzustandsbestimmung an erster Stelle. Für die MS- und NS-Netzzustandsbestimmung laufen aktuell diverse Forschungsprojekte, wie z.B. das Projekt Redispatch 3.0[10]. Besonders vielversprechend erweist sich dabei die Netzzustandsbestimmung mittels künstlicher neuronaler Netze, die in Kapitel 5.2.1 als erster Use Case beispielshaft durchlaufen wird. Neben der MS-Netzzustandsbestimmung nehmen Energie-Prognosen eine entscheidende Rolle ein. Akkurate Einspeise- und Verbrauchsprognosen dienen vielfach als Grundlage für weiterführende Anwendungen, wie z.B. Hochrechnungen, Redispatch2.0 und insbesondere auch für die Netzzustandsbestimmung, welche dann zu einer Netzzustandsprognose wird. Während Erzeuger, speziell Wind und PV als gut prognostizierbar gelten, sind Verbrauchsprognosen deutlich schwieriger zu erstellen und wurden von den Netzbetreibern als eine Herausforderung beschrieben, in der sie Forschungsbedarf sehen. Als zweiter Anwendungsfall, für den beispielhaft der Leitfaden durchlaufen wird, wurde daher der Anwendungsfall aus Challenge 3 des praktischen Data4Grid-Projektteils gewählt: KI-gestützte Verbrauchsprognosen auf Basis von Smart-Meter-Daten. Hierbei wurde untersucht inwieweit sich präzise Verbrauchsprognosen auf Basis von Smart-

[10] https://www.offis.de/offis/projekt/rd30.html

Meter Daten ableiten lassen (siehe auch *Challenge 3: KI-gestützte Verbrauchsprognosen auf Basis von Smart-Meter-Daten* im Data4Grid Projektbericht).

Die ersten beiden Use Cases befinden sich aktuell noch in der Forschungsphase, weshalb als dritter Anwendungsfall ein Beispiel gewählt wurde, das bereits erfolgreich in der Praxis umgesetzt wurde und konkrete Antworten auf viele der definierten Leitfragen geben kann. Die Wahl fiel auf die von MITNETZ STROM entwickelte und im Rahmen der Workshops vorgestellte Anwendung des Frühwarnsystems für Störungen in Umspannwerken, das auf Künstlicher Intelligenz basiert.

5.2.1 Leitfaden für die Netzzustandsbestimmung mit neuronalen Netzen

Mittelspannungsnetze besitzen aufgrund ihrer historisch gewachsenen Struktur nur eine geringe Anzahl an Messeinrichtungen für die Erfassung von sicherheitsrelevanten Variablen. Meist werden lediglich an den HS/MS-Umspannstationen sowie an vereinzelten MS/NS-Ortsnetzstationen Systemgrößen wie Leitungsstrom, Spannungsbetrag, Wirk-, und Blindleistung erfasst. Außerhalb dieser gemessenen Werte ist der Zustand des Stromnetzes unbekannt. Dies führt in Verbindung mit dem voranschreitenden Ausbau dezentraler Erzeugungsanlagen dazu, dass mögliche Grenzwertverletzungen, wie Unter- oder Überschreitungen des zulässigen Spannungsbandes oder Betriebsmittelüberlastungen durch zu hohe Ströme, nicht vollständig identifiziert und lokalisiert werden können. Neben analytischen Verfahren zur Zustandsschätzung (WLS, LP) können Methoden, die mithilfe künstlicher neuronaler Netze die elektrischen Variablen schätzen, zur Erhöhung der Transparenz in der Mittelspannungsebene beitragen. Hierdurch wird bspw. die Möglichkeit geschaffen, dass Betriebsmittel näher an ihren Grenzen betrieben werden können, um kostenintensiven Netzausbaumaßnahmen entgegenzuwirken. Im Folgenden wird der Leitfaden beispielhaft für die Netzzustandsbestimmung mittels künstlicher neuronaler Netze durchlaufen.

Schritt 1: Entscheidungspfade, Machbarkeitsanalyse und Mehrwert

Allgemein

Mehrwert der Anwendung

- Bestimmung des vollständigen Netzzustands, wodurch Netztransparenz generiert wird
  - Erkennung und Vermeidung von Grenzwertverletzungen
  - Nutzung zur Netzwiederversorgung z.B. nach Kurzschlüssen
  - Ermittlung von Flexibilitäten, die z.B. für die Verwendung von Optimierungen eingesetzt werden können
- Geringere Investitionen in zusätzliche Messinfrastruktur

Definition von Verantwortlichkeiten im Unternehmen & Bestimmung der Umsetzungsart

- Fragen zur Art der Umsetzung (intern/ extern) und Verantwortlichkeiten müssen unternehmensspezifisch beantwortet werden. Die im Leitfaden definierten Fragen können hierbei als Hilfe dienen.

Daten	**Bewertung der zur Verfügung stehenden Daten und Ressourcen** - Welche Daten und Ressourcen aktuell zur Verfügung stehen unterscheiden sich je nach Unternehmen und müssen vor Ort evaluiert werden.
	Welche Datenarten werden für die Anwendung benötigt? - Ein rechenfähiges Netzmodell - Last- und Erzeugungsdaten - Historische Messzeitreihen **Müssen neue Messstellen oder Sensorik eingerichtet werden?** - Messstellendichte für geforderte Schätzgenauigkeit ausreichend? - Optimale Messstellenplatzierung: Wo werden neue Messstellen platziert? **Erfordert der beabsichtigte Use Case eine Datenerfassung in Echtzeit?** - Bereitstellung der Messdaten in Echtzeit (Zeitliche Auflösung der Echtzeitdaten z.B. 5 min, 15 min)
Anwendung/ Methode	**Bewertung der Anforderungen an die Systemverfügbarkeit** - Hohe Systemverfügbarkeit von Echtzeitmessdaten aus SCADA System erforderlich.
	Bestimmung der Methode und ihrer Durchführbarkeit - Die Netzzustandsbestimmung mit neuronalen Netzen wird bereits in verschiedenen Forschungsprojekten untersucht und an Netzabschnitten beispielhaft getestet
Regulat. Rahmen	**Prüfung der rechtlichen Rahmenbedingungen** - Bei der Nutzung von Kundendaten für Lastprofile muss der Datenschutz beachtet werden.

Tabelle 11: Schritt 1 des Implementierungsleitfadens am Beispiel der Netzzustandsbestimmung mit neuronalen Netzen.

Schritt 2: Planung

Allgemein	**Ressourcen-, Personal- und Kostenplanung** - Die Ressourcen-, Personal- und Kostenplanung muss unternehmensspezifisch erfolgen.
Daten	**Präzise Festlegung der konkreten Datenanforderungen** - **Vollständig rechenfähiges Netzmodell mit Geokoordinaten** Mögliche Datenmodelle: Siemens PSS Sincal, DIgSILEND PowerFactory, CIM, pandapower.

Daten

Bestehend aus:

- Topologischen Daten
- Daten der Betriebsmittel (Leitungsimpedanzen, Transformatoren usw.)
- EEG/DEA Anlagen (Nennleistung, Anschlusspunkt, Typ)
- Konventionellen Erzeugungsanlagen (Nennleistung, Anschlusspunkt, Typ)
- Lasten/Verbraucher (Nennleistung, Anschlusspunkt, Typ)

Historische Messzeitreihen

- Datenformat: z.B. MS Excel, CSV, TXT, JSON
- Zeitliche Auflösung: max. 15 min (empfohlen: 5 min, 10 min)
- Länge der Zeitreihen: mind. 1 Jahr (empfohlen: 2-4 Jahre)

Einspeisezeitreihen

- PV: Einspeiseleistung von Referenzanlage(n)
- Wind: Einspeiseleistung von Referenzanlage(n)
- Biogas: Einspeiseleistung von Referenzanlage(n)
- Sonstige: Einspeiseleistung von z.B. konventionellen Erzeugern/Kraftwerken

Lastzeitreihen

- Messdaten aus dem HS/MS Umspannwerk (UW)
- Messungen der MS Sammelschienenabgänge
- Messungen der HS/MS Transformatoren
- Messdaten aus Ortsnetzstationen (MS/NS)
- Messdaten von Kundenlasten (z.B. Lastgänge von Großkunden)

Lastprofile (falls keine historischen Messdaten verfügbar):

- Annahmen für Lastprofile (z.B. Standardlastprofile H0, G0, Wärmepumpen usw.)

Daten der Messgeräte

- Typ der Messung*
- Ort/Platzierung der Messung*
- Messrauschen bzw. Genauigkeitsklasse (Herstellerdatenblatt)

Schalterstellungen

- Schalterstellungen der MS-Abgänge im HS/MS Umspannwerk (UW)
- Schalterstellungen der Sammelschienen im UW
- Schalterstellungen von Trennstellen im Netzgebiet an Ortsnetzstationen (ONS) und Kabelverteilerschränken (KVS)
- Position des Trafostufenstellers der HS/MS Transformatoren im UW
- Position der Trafostufensteller der MS/NS Transformatoren in der ONS (z.B. bei RONTs)

**Zuordnung von Platzierung und Typ der Messung im Netzmodell kann auch über die Angaben in den historischen Messzeitreihen erfolgen.*

Anwendung/ Methode	**Präzise Definition des Vorgehens und des Ziels der Methode** - Ziel: Zustandsschätzung des gesamten MS/NS Netzgebiets (unter Nutzung vorhandener Messstellen). - Methodik: Künstliche Neuronale Netze 1. Erzeugung von Trainingsdaten. 2. Training künstlicher neuronaler Netze. 3. Schätzung des Netzzustands auf Basis von Echtzeit-Messungen
Regulat. Rahmen	**Erstellung von Verträgen, detaillierte Prüfung der Rechtsabteilung** - Sollte die Durchführung mit Drittanbietern oder Partnern stattfinden, müssen entsprechende Verträge geschlossen werden.

Tabelle 12: Schritt 2 des Implementierungsleitfadens am Beispiel der Netzzustandsbestimmung mit neuronalen Netzen.

Schritt 3: Durchführung & Validierung

Allgemein	**Ergebnisdarstellung** - Für die Netzzustandsbestimmung könnten Benachrichtigungen denkbar sein, die auf drohende Grenzwertverletzungen hindeuten sowie die farbige Darstellung der Ergebnisse über eine Einfärbung der Netztopologie.
Daten & Anwendung/ Methode	**Entwicklung, Training & Optimierung** - Zur Netzzustandsbestimmung sind bereits verschiedene Methoden vorhanden, je nach Methode unterscheidet sich das Training. **Validierung** - Für die Netzzustandsbestimmung eignet sich die Validierung anhand von realen Messungen, wenn für das Training nicht alle vorhandenen Messstellen genutzt wurden und die geschätzten Ergebnisse mit den Messwerten der ungenutzten Messstellen verglichen werden können.
Regulat. Rahmen	**Beachtung des regulatorischen Rahmens** - Speziell bei dem Einsatz von KI-Methoden sollten sich ändernde rechtliche Rahmenbedingungen verfolgt und eingehalten werden.

Tabelle 13: Schritt 3 des Implementierungsleitfadens am Beispiel der Netzzustandsbestimmung mit neuronalen Netzen.

Schritt 4: Inbetriebnahme

Allgemein	**Integration in bestehende Systeme und den operativen Betrieb** - Die Anwendung für die Netzzustandsbestimmung muss in die Leitwarte integriert werden. Auf den Rechnern/Clouds in der Leitwarte werden lokal neuronale Netze liegen (auch schon in der Validierungsphase), die die Messdaten empfangen und eine Schätzung generieren.
Allgemein	**Transparenz & Akzeptanz im Unternehmen schaffen** - Eine Schulung des Personals ist wichtig, damit es mit der Ergebnisdarstellung umgehen kann.
Daten & Anwendung/ Methode	**Einführung der Anwendung** - Abhängig von verschiedenen Faktoren, z.B. je nach eingesetzten Systemen und Software, können die Herausforderungen bei der Inbetriebnahme je nach Unternehmen stark variieren, sodass hier keine konkreten Angaben erfolgen können.
Regulat. Rahmen	**Beachtung des regulatorischen Rahmens** - Speziell bei dem Einsatz von KI-Methoden sollten sich ändernde rechtliche Rahmenbedingungen verfolgt und eingehalten werden.

Tabelle 14: Schritt 4 des Implementierungsleitfadens am Beispiel der Netzzustandsbestimmung mit neuronalen Netzen.

Schritt 5: Wartung und Weiterentwicklung

Allgemein	**Auswertung der Wirkung und des Mehrwerts der Anwendung** - Konnte die angestrebte Schätzgenauigkeit durch Validierungsmessungen über einen langen Zeitraum sichergestellt werden? - Wurden Kosteneinsparungen durch die Anwendung der Methodik erzielt? - Feedback der Anwender: Wurden durch die Sichtbarkeit der Schätzergebnisse vorbeugende Schalthandlungen durchgeführt? Ist der Mehrwert für das Personal ersichtlich geworden?
Daten & Anwendung/ Methode	**Datendrift identifizieren und reagieren** - Neue, unbekannte Zustände können nicht geschätzt werden. Die neuronalen Netze müssen kontinuierlich nachtrainiert werden, um auch neue Zustände schätzen zu können - Standardlastprofile verändern sich, sodass diese aktuell gehalten werden müssen, z.B. durch entsprechende KI-Methoden, die automatische Anpassungen ermöglichen

Regulat. Rahmen	**Gibt es Änderungen des regulatorischen Rahmens, die Einfluss auf die Anwendung nehmen?** Speziell bei dem Einsatz von KI-Methoden sollten sich ändernde rechtliche Rahmenbedingungen verfolgt und eingehalten werden.

Tabelle 15: Schritt 5 des Implementierungsleitfadens am Beispiel der Netzzustandsbestimmung mit neuronalen Netzen.

Die Netzzustandsschätzung mittels künstlicher neuronaler Netze ist ein vielversprechender Ansatz zur Schaffung von Transparenz in der Mittelspannungsebene. Bisherige Testphasen hierzu haben gezeigt, dass die geschätzten elektrischen Variablen (Leitungsstrom, Wirkleistungsfluss, Spannung) im überwiegenden Teil des Testzeitraums nur eine geringe Abweichung zu den realen Messreihen aufweisen. Besondere Aufmerksamkeit liegt auf der Erstellung der Trainingsdaten, hier muss eine möglichst präzise Abbildung von Industrielasten und dezentralen Erzeugungsanlagen anhand ihrer individuellen Zeitreihen erfolgen, um möglichst genaue Ergebnisse zu erhalten. Werden alle Kriterien berücksichtigt, erhalten Netzbetreiber nach einem erfolgreichen Durchlauf der beschriebenen fünf Schritte eine Anwendung, die zur Sichtbarkeit in ihrem Netzbereich verhilft und neben der Erkennung und Vermeidung von Grenzwertverletzungen weiteres Potential bietet, z.B. bei der Netzwiederversorgung nach Kurzschlüssen. Weiterhin sind Kosteneinsparungen durch den vermiedenen Zubau von Messinfrastruktur sowie Netzausbaumaßnahmen durch die Anwendung eines Verfahrens zur Zustandsschätzung möglich.

5.2.2 Leitfaden für KI-basierte Verbrauchsprognosen

Zur Vorhersage des Stromverbrauchs von kleinen und mittleren Verbrauchern werden bisher vor allem Standardlastprofile verwendet. Allerdings verändert sich das Verbrauchsverhalten durch die Nutzung von selbst erzeugtem Strom und neuartigen Verbrauchen wie E-Kfz und Wärmepumpen derzeit dramatisch. Dieses veränderte Verbrauchsverhalten kann durch Standardlastprofile nicht mehr ausreichend genau modelliert werden. Akkurate Prognosen des Stromverbrauchs von Haushalten und Gewerbebetrieben sowie von Ladestationen für Elektroautos und weiteren Verbrauchern werden daher in Zukunft ein elementarer Baustein sein, um auch bei schwankenden Einspeiseleistungen einen stabilen Netzzustand garantieren zu können. Mit der vermehrten Installation von Smart Metern steigt die verfügbare Datenmenge kontinuierlich, wodurch, insbesondere durch die hohe Granularität der Daten, eine gute Basis für Lastprognosen in Verteilnetzen geschaffen werden kann. Im Folgenden wird der Leitfaden beispielhaft für eine Methode durchlaufen, die Verbrauchsprognosen auf Basis von Smart Meter-Daten mithilfe von KI-Verfahren erstellt.

Schritt 1: Entscheidungspfade, Machbarkeitsanalyse und Mehrwert

Allgemein

Mehrwert der Anwendung

- Deutliche Verbesserung gegenüber Standardlastprofilen, da individuelle Prognosen erstellt werden und kein Durchschnitt einer Verbrauchergruppe prognostiziert wird
- Wesentlicher Input für Netzzustandsbestimmungen bzw. Prognosen
- Ermöglicht proaktiven Netzbetrieb (z.B. Abschaltung von Verbrauchern)

Definition von Verantwortlichkeiten im Unternehmen & Bestimmung der Umsetzungsart

- Fragen zur Art der Umsetzung (intern/ extern) und Verantwortlichkeiten müssen unternehmensspezifisch beantwortet werden. Die im Leitfaden definierten Fragen können hierbei als Hilfe dienen.

Daten

Bewertung der zur Verfügung stehenden Daten und Ressourcen

- Welche Daten und Ressourcen aktuell zur Verfügung stehen unterscheiden sich je nach Unternehmen und müssen vor Ort evaluiert werden.

Anforderungen an die Datenerfassung: Welche Datenarten werden für die Anwendung benötigt?

- Historische Messzeitreihen der zu prognostizierenden Verbraucher (zum Training der KI-Modelle und ggfs. zur Evaluierung)
- Live-Messwerte der zu prognostizierenden Verbraucher als Eingangsgröße für die KI-Modelle (nicht zwingend notwendig, erhöht jedoch die Prognosegüte)
- Weitere Eingangsgrößen bzw. erklärende Variablen für die KI-Modelle (abhängig von der Art des Verbrauchs), z.B. Zeit- und Kalenderinformationen (Tageszeit, Wochentag, Feiertag, etc. → können durch Prognosesystem selbst erzeugt werden), Wetterprognosen (z.B. Temperatur, solare Einstrahlung: je nach Wettermodell kostenpflichtig oder kostenfrei: ICON vom Deutschen Wetterdienst DWD)
  - ➢ Entscheidend für die Erstellung von Verbrauchsprognosen basierend auf KI-Modellen ist das Vorhandensein von historischen Messzeitreihen als Trainingsgrundlage. Meist basieren diese Messzeitreihen auf RLM- oder Smart-Meter-Messungen.

Anwendung/ Methode

Bewertung der Anforderungen an die Systemverfügbarkeit

- Zur Sicherstellung der durchgängigen Systemverfügbarkeit bietet es sich an, redundante Systeme zur verwenden.
- Um jederzeit Verbrauchsprognosen erzeugen zu können, muss eine Ersatzwertbildung für fehlenden Eingangsdaten gewährleistet sein bzw. können Ersatzmodelle verwendet werden, die zum Einsatz kommen, wenn bestimmte Eingangsgrößen wie z.B. Messungen nicht zur Verfügung stehen.

Anwendung/ Methode	**Bestimmung der Methode und ihrer Durchführbarkeit** - Die Erstellung von Leistungsprognosen (z.B. für Windenergie und PV) basierend auf KI-Modellen ist State-of-the-Art und seit vielen Jahren etabliert. Auch Verbrauchsprognosen werden seit einigen Jahren auf diese Art erzeugt. - Je nach Anwendungsfall können unterschiedliche KI-Modelle verwendet werden. Geht es vor allem um Leistungsspitzen einzelner Verbraucher müssen andere Methoden verwendet werden als bei der Prognose des Verbrauchs einer größeren Verbrauchergruppe.
Regulat. Rahmen	**Prüfung der rechtlichen Rahmenbedingungen** - Bei der Nutzung von Verbrauchsmessungen handelt es sich oft um personenbezogene Daten, daher müssen Datenschutz und Datensicherheit in besonderem Maße beachtet werden.

Tabelle 16: Schritt 1 des Implementierungsleitfadens am Beispiel der Anwendung für KI-basierte Verbrauchsprognosen.

Schritt 2: Planung

Allgemein	**Ressourcen-, Personal- und Kostenplanung**
	- Die Ressourcen-, Personal- und Kostenplanung ist vor allem von der Entscheidung abhängig, welche der folgenden beiden Optionen gewählt wird:
	  ➢ Option 1: Interne Erstellung der Prognosen evtl. durch externe Unterstützung. Infrastruktur muss geschaffen werden (z.B. Server), Personal mit Kenntnissen in Data-Analysis und Erfahrung in der Prognoseerstellung wird benötigt, Prozesse müssen aufgesetzt werden. Hoher Aufwand, insbesondere, wenn ähnliche Prozesse (noch) nicht im Unternehmen existieren.
	  ➢ Option 2: Externe Erstellung der Prognosen durch Prognoseanbieter. Der Aufwand beschränkt sich auf die Bereitstellung der historischen Messwerte sowie Stammdaten. Beachtung der erhöhten Datenschutzanforderungen, geringere Kontrolle für die Daten, geringer interner Aufwand. Kosten abhängig von Anzahl der Prognosen und Art der benötigten Prognose (z.B. Short-Term, Day-Ahead).
	- Es werden wenige externe Daten benötigt, Wetterprognosen können kostenlos vom Deutschen Wetterdienst beschafft werden.

Daten	**Präzise Festlegung der konkreten Datenanforderungen** - Historische (und ggfs. live-) Messzeitreihen des Verbrauchs, zeitliche Auflösung 15 Minuten, je nach Anwendungsfall auch höher (z.B. 1 Minute). - Einheitlicher Export oder Bereitstellung via Schnittstelle. - Falls verfügbar und mit DSVGO vereinbar: Metadaten zur Verbrauchsstelle, z.B. Art des Verbrauchers (Haushalt, Industriebetrieb, Büro…), Elektroauto oder Wärmepumpe vorhanden, etc.

Daten	✚ Datenbereinigung: Erkennung und Bereinigung von konstanten Werten („Datenhänger“), Ausreißern, etc. ✚ Diverse Eingangsgrößen (abhängig von Verbrauchstyp) für die KI-Modelle in zu prognostizierender zeitlicher Auflösung.
Anwendung/ Methode	**Präzise Definition des Vorgehens und Ziels der Methode** ✚ Ziel: Prognose des Stromverbrauchs bestimmter Verbraucher auf Basis von historischen Messungen für die nächsten Stunden und Tage. ✚ Methodik: Training von Machine-Learning-Modellen auf historischen Daten und Anwendung dieser Modelle auf Eingangsdaten zur Erzeugung von Prognosen.
Regulatorischer Rahmen	**Erstellung von Verträgen, detaillierte Prüfung der Rechtsabteilung** ✚ Beachtung der DSVGO, insbesondere in Bezug auf personenbezogene Verbrauchsmesszeitreihen. ✚ Sollte die Durchführung mit Drittanbietern oder Partnern stattfinden, müssen entsprechende Verträge geschlossen werden.

Tabelle 17: Schritt 2 des Implementierungsleitfadens am Beispiel der Anwendung für KI-basierte Verbrauchsprognosen.

Schritt 3: Durchführung & Validierung

Allgemein	**Ergebnisdarstellung** ✚ Die Verbrauchsprognosen liegen in der Regel nach Erstellung als Zeitreihen beispielsweise für die nächsten 96 Viertelstunden vor in einem definierten Format an einer Schnittstelle oder in Form einer Datei vor. ✚ Falls für den Anwender hilfreich kann auch eine grafische Darstellung der Prognosen realisiert werden (s. Option 2, Validierung).
Daten & Anwendung/ Methode	**Entwicklung, Training & Optimierung** ✚ Für die Prognoseerstellung existieren verschiedene Methoden. In der Regel findet ein Training der Modelle auf historischen Daten statt, das regelmäßig wiederholt wird. Die automatisierte Prognoseerstellung (Prognosen für neue Prognoseobjekte) sowie ein kontinuierliches Training der Modelle werden immer häufiger. ✚ Messwerte als Eingangsgrößen für die Machine-Learning-Modelle erhöhen die Prognosequalität sind jedoch auch mit der höchsten Wahrscheinlichkeit nicht verfügbar. Hier ist es möglich, entweder Ersatzwerte zu bilden oder ein Back-Up-Modell zu verwenden, das keine Messwerte als Eingangsgröße verwendet.

Daten & Anwendung/ Methode	**Validierung**
	- Zur Validierung der Prognosegüte gibt es vor allem 2 Optionen:
	  - Option 1: Berechnung von Fehlermaßen (z.B. des quadratischen Fehlers RMSE). Diese Option bieten einen guten Überblick – insbesondere bei einer großen Anzahl an Prognosen
	  - Option 2: Darstellung der Prognosen gegenüber der Messung. Diese Option bietet die Option zur vertieften Analyse der Prognosegüte.

Tabelle 18: Schritt 3 des Implementierungsleitfadens am Beispiel der Anwendung für KI-basierte Verbrauchsprognosen.

Schritt 4: Inbetriebnahme

Allgemein	**Integration in bestehende Systeme und den operativen Betrieb** - Für die Inbetriebnahme ist entscheidend, dass ein ausgereiftes Datenmanagement vorhanden ist, das notwendige Daten, insbesondere die historischen Messzeitreihen, in definierten Schnittstellen für die Anwendung bereitstellt.
	Transparenz & Akzeptanz im Unternehmen schaffen - Eine Schulung des Personals ist wichtig, damit diese im Umgang mit Prognosen – in Bezug auf die Erstellung aber auch auf die Verwendung – vertraut sind.
Daten & Anwendung/ Methode	**Einführung der Anwendung** - Abhängig von verschiedenen Faktoren, z.B. je nach eingesetzten Systemen und Software, können die Herausforderungen bei der Inbetriebnahme je nach Unternehmen stark variieren, sodass hier keine konkreten Angaben erfolgen können.
Regulat. Rahmen	**Beachtung des regulatorischen Rahmens** - Speziell bei dem Einsatz von KI-Methoden sollten sich ändernde rechtliche Rahmenbedingungen verfolgt und eingehalten werden.

Tabelle 19: Schritt 4 des Implementierungsleitfadens am Beispiel der Anwendung für KI-basierte Verbrauchsprognosen.

Schritt 5: Wartung & Weiterentwicklung

Allgemein	**Auswertung der Wirkung und des Mehrwerts der Anwendung** - Der Vorteil der Verbrauchsprognosen zeigt sich insbesondere im Vergleich zu bisher verwendeten Methoden wie Standardlastprofilen. Der Mehrwert zeigt sich in den Anwendungen, die auf den Verbrauchsprognosen aufbauen, wie z.B. Netzzustandsschätzungen. Hierbei können beispielsweise im Vorhinein erkannte Überlastungen von Betriebsmitteln etc. bewertet werden.

Daten & Anwendung/ Methode	**Datendrift identifizieren und reagieren** - Die Anzahl der vermessenen Verbraucher wird in den nächsten Jahren ständig anwachsen, daher ist die Aufnahme neuer Prognoseobjekte sowie regelmäßiges Nachtraining unerlässlich. Zudem muss die Skalierbarkeit des Systems berücksichtigt werden.
Regulat. Rahmen	**Gibt es Änderungen des regulatorischen Rahmens, die Einfluss auf die Anwendung nehmen?** - Speziell bei dem Einsatz von KI-Methoden sollten sich ändernde rechtliche Rahmenbedingungen verfolgt und eingehalten werden.

Tabelle 20: Schritt 5 des Implementierungsleitfadens am Beispiel der Anwendung für KI-basierte Verbrauchsprognosen.

Prognosen für die Erzeugung, den Verbrauch und Leistungsflüsse sind ein wichtiger Baustein für mehr Transparenz im Verteilnetz. Präzise Prognosen bilden zudem die Grundlage für etliche wietere Anwendungen wie beispielsweise die Netzzustandsschätzung (siehe Kapitel 5.2.1). In dem zuvor beschriebenen Use Case konnten auf der Grundlage von Smart Meter Daten Verbrauchsprognosen erstellt werden, die das individuelle Verhalten der Verbraucher deutlich realistischer abbilden als dies durch Standardlastprofile möglich ist. Dabei konnte festgestellt werden, dass sich eine Veränderung der Standardlastprofile abzeichnet. So kommt es u.a. bereits zu Verschiebungen der Spitzenlasten oder zur Bildung neuer Peaks. Es ist lohnenswert für Netzbetreiber Smart Meter Daten zu nutzen und z.B. die Schritte zur Umsetzung dieses Use Cases zu durchlaufen. In Verbindung mit weiteren Datensätzen, z.B. zu exogenen Einflüssen, können Netzbetreiber schließlich eine Anwendung erhalten, die auch die schwer vorhersagbaren Spitzenlasten besser prognostizieren kann.

5.2.3 Leitfaden für ein KI-basiertes Frühwarnsystem für Störungen in Umspannwerken

Die Mitteldeutsche Netzgesellschaft Strom mbH (MITNETZ STROM) hat als erster Netzbetreiber in Deutschland ein KI-basiertes Frühwarnsystem für Störungen in Umspannwerken entwickelt. Ein Grund für die Entwicklung einer solchen Anwendung waren mehrere schwere Schäden an Umspannwerken, die Kosten in Millionenhöhe zur Folge hatten. Mehrere tausend Kunden waren über Stunden ohne Strom. Vor diesem Hintergrund kam die Frage auf, ob Vorsorgemaßnahmen ergriffen werden können, um schwere Schäden und Versorgungsausfälle in Folge verhindern zu können, beispielsweise durch eine frühzeitige Erkennung.

Für die Anwendung werden verschiedene Daten, u.a. Netzdaten und Betriebsmittelzustände, mit der Fehlerhistorie von Umspannwerken verknüpft, um Hinweise auf eventuell eintretende Störungen zu erhalten. Die Ergebnisse der Analyse werden als Monatsberichte an das Anlagen-Management und den Netzbetrieb gesendet. Werden Komponenten als auffällig gekennzeichnet, kann eine frühzeitige Prüfung und ggf. schnelle Instandsetzung durchgeführt werden. In der folgenden Tabelle werden die einzelnen Schritte des Leitfadens beispielhaft für die Entwicklung des Frühwarnsystems von MITNETZ STROM durchlaufen, um die konkrete Vorgehensweise praxisnah zu beschreiben.

Schritt 1: Entscheidungspfade, Machbarkeitsanalyse und Mehrwert

Allgemein	**Mehrwert der Anwendung**
	- Frühzeitige Erkennung von möglichen Schäden an Umspannwerken.
	  ➢ Gezielte bedarfsorientierte Planung und schnelle Durchführung von Instandhaltungsmaßnahmen.
	  ➢ Vermeidung von Schäden an Umspannwerken und daraus resultierenden Versorgungsausfällen.
	  ➢ Kosteneinsparungen!

	Definition von Verantwortlichkeiten im Unternehmen - MITNETZ STROM besitzt eine eigene Abteilung zur Entwicklung von innovativen Anwendungen. An der Entwicklung der Anwendung beteiligt sind das Asset-Management, die IT-Systementwicklung und interne Data Scientists. - Im Rahmen der Entwicklung wurden u.a. die Rollen des Product Owners , Stakeholder (z.B. Bereichsleiter, CEO, Asset Management Kollegen) und Entwickler (Data Scientists), vergeben.
	Bestimmung der Umsetzungsart - Das Projekt wird intern bei MITNETZ STROM durchgeführt, bei der Daten-Analyse wird mit der Unternehmensberatung McKinsey zusammengearbeitet.
Daten	**Bewertung der zur Verfügung stehenden Daten und Ressourcen** - MITNETZ STROM verfügt über einen großen Datenschatz und hat eine moderne Dateninfrastruktur aufgebaut, die für Analysen zur Verfügung steht.
	Anforderungen an die Datenerfassung - Für die Anwendung sind Netzdaten, Betriebsmitteldaten, Fehlerhistorien und externe Wetterdaten notwendig, die miteinander verknüpft werden müssen.
Anwendung/ Methode	**Bewertung der Anforderungen an die Systemverfügbarkeit** - Eine Systemunterbrechung kann zu einem hohen technischen/ monetären Schaden führen, der „Good Will“ gegenüber Kunden sinkt

Regulatorischer Rahmen	**Prüfung der rechtlichen Rahmenbedingungen**
	- Genehmigungen müssen in folgenden Bereichen eingeholt werden:
	  ➢ Datensicherheit (Cloud wird genutzt)
	  ➢ Datenschutz (Personenbeziehbare Informationen)
	  ➢ Betriebsrat zur Information

Tabelle 21: Schritt 1 des Implementierungsleitfadens am Beispiel der Anwendung zur KI-basierten Früherkennung von Störungen in Umspannwerken.

Schritt 2: Planung

Allgemein	**Ressourcen-, Personal- und Kostenplanung** - Personaleinsatz: ca. 10 Personen Vollzeit für 4 Wochen - Personalkosten: Wenn nötig sind externe Ressourcen je nach Consulting zu betrachten. - Sonstige Kosten: Kosten für die Cloud (kommt auf den Use Case an), (https://azure.microsoft.com/de-de/pricing/) - Benötigte Ressourcen: Klein starten, bei Bedarf erhöhen der CPU-Kerne, des RAM, etc., Lizenzen für Tableau/ Power BI, alternativ Open Source Lösungen (R-Shiny, Dash, etc.) - Kosten für externe Daten: ca. 2000€ p.a.

Daten	**Datenanforderungen und Datenbereitstellung**
	- Bereitstellung historischer Daten.
	- In die Analyse einbezogen werden:
	  • Anlagendaten, die Informationen zu Standort, Baujahr und Typ einer Schaltanlage geben
	  • Messdaten für die Spannung und Leistung
	  • Betriebsprotokolle (Schalthandlungen)
	  • Daten zu Wartungs- und Instandhaltungsprozessen
	  • Ereignisdaten
	  • Externe Wetterdaten
	- Die einzelnen Daten stammen u.a. aus Systemen wie ACOS, GNet und ProNet.
	- Die Zusammenlegung und Verknüpfung der Daten in einer Datenbank erfolgt als erster Schritt.

Anwendung/ Methode	**Präzise Definition des Vorgehens und des Ziels der Methode** - Ziel ist es, ein Vorhersagemodell zu entwickeln, das den Zustand der Anlagen voraussagt, um potentiellen Fehlerereignissen vorzubeugen. - Auf Basis der Entwicklung soll nicht mehr ereignisorientiert gehandelt werden, d.h. reagiert werden, wenn eine Störung auftritt, sondern mit Hilfe von analytischen Modellen vorausschauend zu agieren. - Im Rahmen der Entwicklung sollen die Daten der vorhandenen internen Systeme verarbeitet und zu einer Datenbank zusammengeführt werden, die anschließend mit Hilfe eines Explorationswerkzeug visualisiert werden können.

Tabelle 22: Schritt 2 des Implementierungsleitfadens am Beispiel der Anwendung zur KI-basierten Früherkennung von Störungen in Umspannwerken.

Schritt 3: Durchführung & Validierung

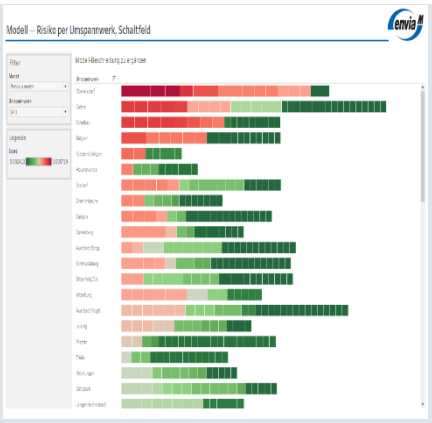
Allgemein

Validierung

- Für die Validierung ist das Asset Management in Form des Forensik Tools (Tableau Dashboard) zuständig.

Ergebnisdarstellung

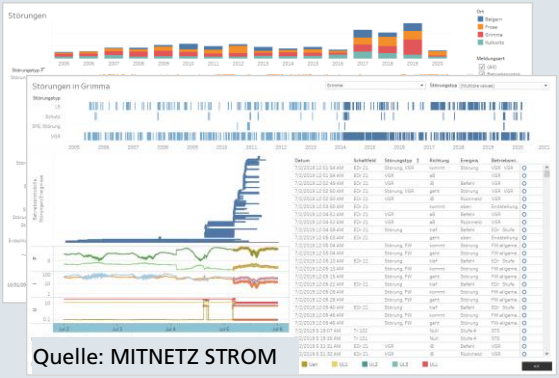
- Ein Dashboard mit Risikoübersicht sowie automatisch generierte E-Mails, in der die riskantesten Schaltfelder und die riskantesten Umspannwerke aufgeschlüsselt werden.
- Ein Link in der E-Mail führt zu einem Analysetool, das die Risikoaufschlüsselung zeigt und die Analyse und Maßnahmenableitung ermöglicht.



Quelle: MITNETZ STROM

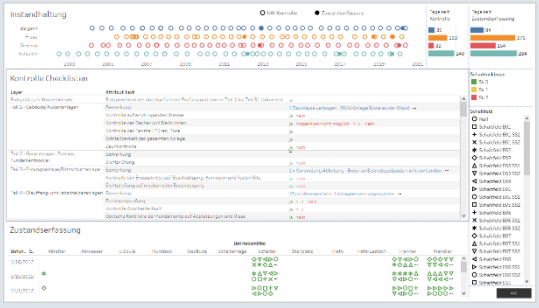
- Mithilfe des Analysetools können die Daten zusätzlich visualisiert werden:

➢ **Zeitreihenanalyse für Störungsforensik:** Integrierte Darstellung der Messwerte sowie aller relevanten Datenquellen rund um ein ausgewähltes Ereignis für die Analysen. Manuelle Extraktion und Filterung werden hierdurch ersetzt.



Quelle: MITNETZ STROM

➢ **Kontroll-Protokolle und Zustandserfassungen zur Planung von Instandhaltungsmaßnahmen:** Interaktiver Abruf zeitlicher Abfolgen und der Protokolle bisheriger Maßnahmen im gleichen Werkzeug.



Quelle: MITNETZ STROM

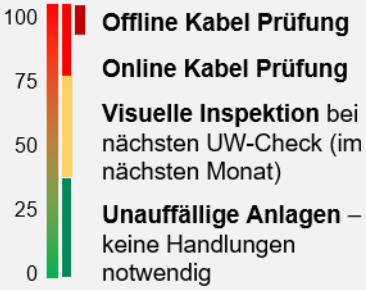
Allgemein	➢ **Asset Management mit grafischen Filtermethoden:** Übersicht des Störungsrisikos auf Basis des integrierten analytischen Modells sowie Auswahl des Umspannwerks und der Schaltfelder anhand grafischer Übersichtskarten zum Einblick in die letzten Störungen.  Quelle: MITNETZ STROM
Daten & Anwendung/ Methode	**Entwicklung, Training & Optimierung** 1. ***Daten***: Nach der Datenverknüpfung erfolgt eine Datenbereinigung und Modellentwicklung auf Abgangsebene und monatsscharf. 2. ***Modell***: Das entwickelte Modell soll Muster zu Ereignissen in den Daten finden. Es erfolgt ein Anlernen der Muster zwischen der Datenbasis und den historischen Schäden. Anschließend die Extrahierung der Erkenntnisse und das Validieren von technischen Hintergründen in den gefundenen Beziehungen. 3. ***Anwendung***: auf der Grundlage der Ergebnisse des Modells werden Handlungsempfehlungen abgeleitet. Auf Basis des Risikowertes wird die passende Handlung abgeleitet und beauftragt.  Quelle: MITNETZ STROM **Validierung** - Expertenwissen des Fachbereichs, Methodische Validierung (AUC/ROC/Var Imp/ SHAP/ etc.).

Tabelle 23: Schritt 3 des Implementierungsleitfadens am Beispiel der Anwendung zur KI-basierten Früherkennung von Störungen in Umspannwerken.

Schritt 4: Inbetriebnahme

Allgemein	**Integration in bestehende Systeme und den operativen Betrieb** - Das Modell generiert eine Bewertung für alle in Betrieb befindlichen SF6 Schaltfelder. - Es ist frei wählbar für welchen Zeitraum in der Zukunft das Modell Störungen vorhersagen soll – je zeitnaher, desto genauer → Das System schaut 1 Jahr nach vorn. Es ist davon abzuraten, diesen Zeitraum zu ändern/ verkürzen (im Zweifel nicht genug Signal in den Daten)

Allgemein	- Aktuell läuft die Risikokalkulation Anfang des Monats, d.h. 7 Tage vor Monatsbeginn wird das Modell ausgeführt und Risikoinformationen extrahiert. - Der Fachbereich nutzt neben dem Forensik Tool ebenfalls eine interne Reporting Lösung, in der die Ergebnisse bereitgestellt werden (niedrigschwellige Bereitstellung der Daten).

Tabelle 24: Schritt 4 des Implementierungsleitfadens am Beispiel der Anwendung zur KI-basierten Früherkennung von Störungen in Umspannwerken.

Schritt 5: Wartung & Weiterentwicklung

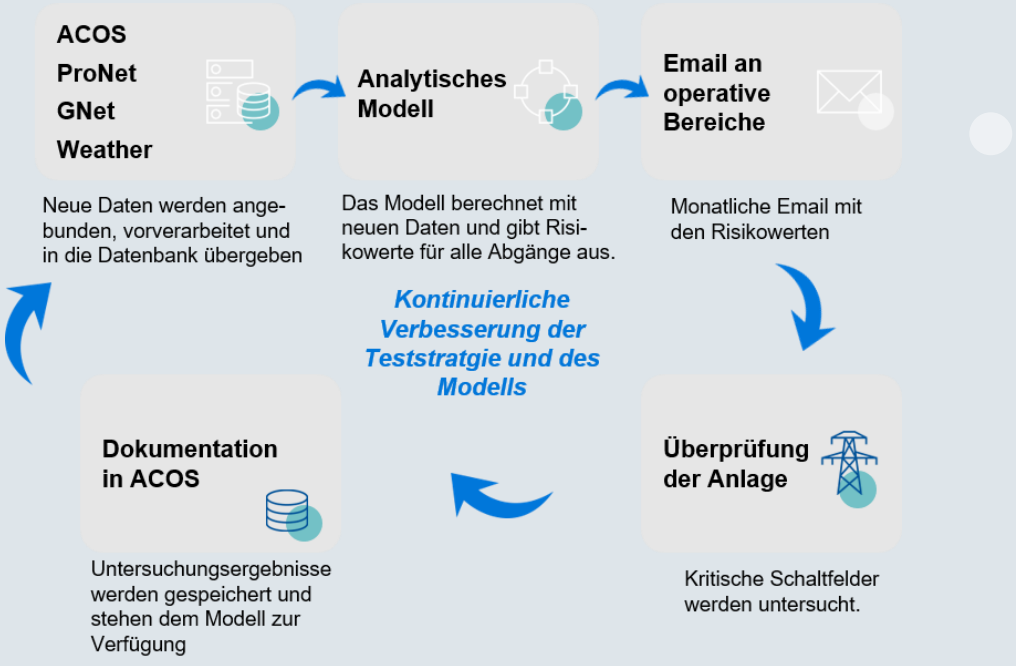
Allgemein

Auswertung der Wirkung und des Mehrwerts der Anwendung

- Das Modell ist sehr vorausschauend und erhöht die Transparenz bei riskanten Vermögenswerten deutlich.
- Das Explorationswerkzeug kann die Bearbeitungsdauer relevanter Anwendungsfälle erheblich reduzieren. → Ermöglicht neue Use Cases, wenn den Kollegen etwas auffällt.

Kontinuierliche Überprüfung und Weiterentwicklung

- Es muss eine kontinuierliche Weiterentwicklung des analytischen Modells durch Etablierung eines Prozesses erfolgen. → Hier werden Metriken aus dem PdM Model genutzt. In dem Moment, in dem sich die AUC verringert, wird eine Neumodellierung empfohlen.
- Die Weiterentwicklung des analytischen Modells erfolgt in Form einer kontinuierlichen Rückkopplungsschleife:



Quelle: MITNETZ STROM

Tabelle 25: Schritt 5 des Implementierungsleitfadens am Beispiel der Anwendung zur KI-basierten Früherkennung von Störungen in Umspannwerken.

Das von MITNETZ STROM entwickelte Frühwarnsystem ist in der Lage mögliche Störungen an Schaltanlagen in den fast 200 Umspannwerken des Unternehmens zu erkennen. Die Anwendung befindet sich bereits in einer erfolgreichen Produktionsphase. Nächste Schritte sind die Umsetzung im Betrieb sowie die Nutzung des Explorationswerkzeugs bei der Risikobewertung im Asset-management. Für die ersten sechs Monate sind Online- und Offline-Prüfungen für alle Hochrisiko-Schaltfelder vorgesehen. Die Ergebnisse dieser Tests sollen anschließend ausgewertet werden und ein zukünftiger Testansatz definiert werden.

6 Evaluation und Ausblick

6.1 Zusammenfassung und Überblick

Die Energiewende stellt vor allem die Stromverteilernetze vor neue An- und Herausforderungen, da sich die Komplexität durch die Integration vieler dezentraler Erzeugungsanlagen sowie die Einbindung von flexiblen Lasten und Speichern bedeutend erhöht. Die Digitalisierung von Informationen und deren Verarbeitung sowie die Automatisierung von wiederkehrenden Prozessen, insbesondere im Bereich Datenmanagement, öffnen dabei Türen für neue Möglichkeiten, um die steigende Komplexität zu beherrschen. Digitale Technologien wie z.B. Datenaustauschplattformen und innovative Anwendungen mit Nutzung von künstlicher Intelligenz wie z.B. vorrausschauendes Wartungswesen, können dabei unterstützen, Prozesse effizienter zu gestalten und Abläufe zu optimieren. Zusätzlich können aber auch komplett neue Anwendungen realisiert werden, die mit bisherigen Methoden und der aktuellen Datengrundlage nicht möglich waren (Beispiel: KI-Netzzustandsbestimmung oder Energieprognosen. Siehe hierzu auch Kapitel 2 und Tabelle 2).

Gleichzeitig steigen aber auch die Risiken von Fehlern durch die verstärkte Nutzung von Informations- und Kommunikationstechnologien im Stromnetz, wenn der Betrieb auf datengetriebenen Prozessen basiert und die Datengrundlage nicht valide ist. Zudem ist eine ganzheitliche Sicherheitsbetrachtung der informationstechnischen Systeme notwendig, die die Einhaltung eines angemessenen Datenschutz- und Sicherheitsniveaus gewährleistet.

Im Rahmen dieses Gutachtens wurden dazu in Kapitel 2 datengetriebene Prozesse im Umfeld einer kritischen Infrastruktur, wie bei den Stromnetzbetreibern, betrachtet. Hier konnte identifiziert werden, dass gerade durch die wechselseitige Abhängigkeit von Stromnetz und Energieversorgung auf der einen Seite und der Informations- und Kommunikationsinfrastruktur auf der anderen Seite besondere Vorsicht geboten ist. Datengetriebene Prozesse und Anwendungen benötigen besondere Beachtung in Hinblick auf mögliche Konsequenzen bei fehlerhaften oder unterbrochenen Prozessen des jeweils andern Feldes. Ein Datenausfall kann prinzipiell zu einem Stromausfall führen, der wiederrum zu weiteren Datenausfällen führen kann. Möglichkeiten wie man die Kritikalität der Prozesse in den verschiedenen Bereichen des Netzbetriebes anhand von definierten Indikatoren einordnen kann, wurden in Abschnitt 2.2 beschrieben. Prozesse, die im Umfeld Netzbetriebsführung und operativer Planung sowie IKT-Sicherheit mit hoher Systemrelevanz und potenzieller IKT-und Datengefährdung stattfinden, besitzen das größte Gefahrenpotential und werden als potenziell kritisch eingeordnet. Prozesse in den Bereichen Instandhaltung und Endkundenbereich sind in der Regel weniger kritisch, da ihre unmittelbaren Auswirkungen deutlich geringer sind. Abschließend wurde in Kapitel 2.3 auf die Verwendung von KI innerhalb datengetriebener Prozesse eingegangen. KI bietet die Möglichkeit bestehende Prozesse effizienter (im Sinne von schneller, genauer und umfassender zu machen), aber auch ganz neue Prozesse und Anwendungen zu realisieren (siehe Tabelle 2 für einen Überblick mit ausgewählten Anwendungen, die KI nutzen und einen Mehrwert für den Netzbetrieb bieten können). Allerdings bringen auch diese Methoden bestimmte Risiken mit sich, die vor dem Hintergrund der kritischen Infrastruktur beachtet werden müssen. Hier wurden insbesondere die Abhängigkeit von der Datengrundlage sowie ein möglicherweise entstehendes zu hohes Vertrauen in die Ergebnisse der KI und die oft fehlenden Möglichkeiten die Ergebnisse nachzuvollziehen identifiziert. Letzteres liegt

einerseits oftmals an dem Black-Box Charakter der KI-Anwendungen aber auch daran, dass Menschen die Entscheidungen der KI nicht mehr rational nachvollziehen können.

Da für alle datengetriebenen und KI-basierten Anwendungen die Daten und ihre Quellen im Vordergrund stehen, wurden in Kapitel 3 neben den dadurch entstehenden Risiken die Themen Datenerfassung, Datenquellen, Datenverfügbarkeit sowie Qualität adressiert. Eine automatisierte Datenerfassung und Archivierung bilden die Grundlage für notwendige Schritte hin zur Digitalisierung von eigenen betrieblichen Prozessen. Um die eigenen Prozesse aber zu erweitern, optimieren oder ganz neu aufzusetzen, ist es oftmals notwendig externe Daten bzw. Informationen mit den eigenen zu korrelieren. Hier wurde festgestellt, dass es neben den öffentlich zugänglichen Daten sehr viele kostenpflichtige Datenquellen gibt und auch Daten die in privater oder unternehmerischer Hand liegen und für die Verwendung in eigenen Prozessen nicht zur Verfügung stehen. An dieser Stelle sei auch noch mal auf die aus wissenschaftlicher Sicht nicht ausreichende Open-Data Mentalität im Bereich der Energieversorgung hingewiesen (unter Berücksichtigung, dass bestimmte strukturelle und personifizierte Daten unbedingt geschützt bleiben müssen). Weiterhin ist zu bemerken, dass die Qualität und Verfügbarkeit eine signifikante Rolle in dem Aufsetzen neuer Prozesse spielen. Hierzu wurde in Kapitel 3.2 auf Basis von Befragungen kleiner und mittlerer VNB eine Einordnung gegeben. Dabei wurde erkannt, dass ein Großteil der benötigten Informationen vorliegt, aber aufgrund mangelnder Dokumentation und Aufwänden bei Export und Überführung in neue Systeme nur eingeschränkt nutzbar ist. Weiterhin sind Daten wie z.B. Lastprofile nicht mehr aktuell und werden mit groben Näherungen an aktuelle Ergebnisse aus Messungen im Netz angepasst. Pauschal lässt sich festhalten, dass die Qualität und Verfügbarkeit der Daten hin zu niedrigeren Spannungsebenen abnehmen. Das lässt sich aus dem historischen verbrauchsdominierten Energiesystem her begründen. Als letzter Punkt wird noch die Expertise bzgl. Datenanalyse und KI sowie ein genereller Mangel an Fachpersonal mit diesen Kompetenzen angeführt. Denn um neue Anwendungen richtig einzuordnen und in ein Unternehmen zu bringen, bedarf es erfahrenem Personal. Dieses muss erst noch in ausreichender Anzahl ausgebildet werden. In Kapitel 3.3 werden die durch die Nutzung von Daten entstehenden Risiken und mögliche Schutzmaßnahmen aufgezeigt. Eine wichtige, wenn auch evtl. triviale Aussage, ist zu realisieren, dass die Datengrundlage für datenbasierte (KI-) Anwendungen in Qualität und Verfügbarkeit ein sehr hohes Niveau haben müssen. Denn, wenn bereits den Eingangsdaten nicht vertraut werden kann, wird das Ergebnis ebenfalls nicht belastbar sein (siehe hierzu auch Abschnitt 2.3.1). Weitere Risiken stellen das Sammeln und Halten der Daten sowie ihr Transport dar. Hier müssen moderne Sicherheitsprotokolle und Zertifikate verwendet werden, um diese Risiken zu minimieren.

Die bisher diskutierten, generellen Anwendungen auf Datenbasis wurden in Kapitel 4 auf mögliche Hindernisse im aktuell geltenden gesetzlichen und regulatorischen Rahmen diskutiert. Hier wurden keine signifikanten Hindernisse identifiziert, wenn auch die Beachtung des Rahmens einen z.T. beachtlichen Aufwand erfordert. Dieser kann wiederrum zu Verzögerungen oder sogar Weglassen von wichtigen Innovationen führen. In Kapitel 5 wurde ein anwendungsnaher Implementierungsleitfaden erstellt, der die verschiedenen technischen und regulatorischen Anforderungen an die Einführung und Umsetzung neuer datengetriebener KI-Anwendungen darstellt und bei Planung, Umsetzung und Betrieb unterstützen soll. Als konkrete Beispiele wurden drei Anwendungen anhand des Leitfadens analysiert.

6.2 Kernaussagen und Handlungsempfehlungen

Derzeit sind im Stromnetz zahlreiche Anwendungsfelder identifiziert, in denen Datenanalysen und KI-Methoden einen erkennbaren Mehrwert für Netzbetreiber generieren können. Unter den großen Netzbetreibern gibt es bereits Vorreiter, die eine solide Dateninfrastruktur aufgebaut haben und erfolgreich datengetriebene Anwendungen nutzen, die zum Teil auf Methoden der künstlichen Intelligenz basieren. E.ON hat als größter Verteilnetzbetreiber in Deutschland angekündigt jährlich 300 – 400 Mio. € in die „Smartifizierung" der Netze zu stecken. Als großer Akteur übernimmt das Unternehmen eine Rolle als Wegbereiter, aus dessen Erfahrungen die kleineren Netzbetreiber lernen können. Im Bereich der Prognose, Netzzustandsschätzung und Elektromobilität laufen bereits verschiedene Projekte zusammen mit Netzbetreibern, die KI-Anwendungen beinhalten. Dennoch müssen aktuell noch viele Hürden für eine flächendeckende Einführung von datengetriebenen Anwendungen überwunden werden. Vor allem kleine Netzbetreiber müssen ihre Datengrundlage verbessern. Als signifikanteste Hürden sind hier mögliche Konsequenzen bei Fehlern oder Abbrüchen in den datengetriebenen Prozessen beim Einsatz in kritischen Infrastrukturen (siehe Kapitel 2.2), die Erfassung, Haltung und Verarbeitung der Daten (siehe Kapitel 3.1) sowie die regelkonforme Verwendung der Daten und Beschreibung neuer Prozesse (siehe Kapitel 4.1) genannt.

Die Kernaussagen und Handlungsempfehlungen, die im Rahmen des Gutachtens erarbeitet wurden, sind im Folgenden noch einmal zusammengefasst.

Daten, Datenanalysen und KI

Datengetriebene Anwendungen bis hin zu KI-Anwendungen haben ein großes Potential, um bestehende Prozesse zu optimieren und neue, bisher nicht mögliche Anwendungen zu realisieren. Sie werden daher im zukünftigen Stromnetz auf allen Netzebenen unerlässlich sein, um der steigenden Komplexität im Stromnetz gerecht zu werden. KI-Methoden können neue Lösungen bereitstellen, die Netzbetreibern einen lohnenswerten ökonomischen Mehrwert bieten und mittel- oder langfristig helfen die Netze transparenter, steuerbarer und stabiler zu machen.

Daten sind der Schlüssel zur Identifikation von Möglichkeiten zur Realisierung eines effizienteren und sichereren Netzes, unabhängig ob KI-Methoden oder herkömmliche Methoden Anwendung finden. Entscheidend für eine erfolgreiche Anwendung ist die Datengrundlage. Kann der Datengrundlage nicht vertraut werden, kann auch den Ergebnissen der Anwendung in Folge nicht vertraut werden. Den Kern einer effizienten Datennutzung bildet eine zentrale Datenhaltung (auch Datendrehscheibe oder Datahub genannt). Sind alle Daten an zentraler Stelle verfügbar, wird die Verknüpfung der einzelnen Daten vereinfacht und die Möglichkeiten für deren Nutzung steigen. Eine Möglichkeit für eine zentrale Datenhaltung wird z.B. durch moderne Datenbanktechnologien gegeben.

Im Status quo ist die Datengrundlage hinsichtlich der Datenmenge und vor allem der Datenqualität im Bereich der Stromverteilnetze in der Mittel- und Niederspannung ungenügend. Besonders Echtzeitdaten stehen sowohl in der Mittel- als auch Niederspannung nicht ausreichend zur Verfügung. Besonders in der Niederspannung erfolgt aktuell partiell noch gar keine Datenerfassung.

Handlungsempfehlung: Analyse und ggf. Verbesserung der Datengrundlage

Damit Netzbetreiber das ihnen zur Verfügung stehende Potenzial voll ausschöpfen können, ist es wichtig, dass sie sich bereits jetzt mit dem Datenbestand innerhalb des Unternehmens auseinandersetzen und die Datengrundlage verbessern. Ein einmaliger, vertretbarer Initialaufwand kann bereits Möglichkeiten schaffen, langfristig zu profitieren. Grundlegende Schritte sollten hierbei sein:

- *Fehlerkorrekturen: Die digitale Netztopologie prüfen und ggf. überarbeiten, d.h. beispielsweise fehlende oder falsch zugeordnete Betriebsmittel ergänzen, um ein rechenfähiges Netzmodell zu erhalten.*
- *Dokumentation von zukünftig potenziell relevanten Informationen (z.B. Schalterstellungen, etc.).*
- *vorhandene Daten verknüpfen (SAP, GIS, …), ggf. durch Einbindung externer Daten (Gebäudeinformationen, Umgebungsinformationen, sozio-demographische Daten).*
- *Internes Know-How aufbauen und pflegen.*

Risiken bei dem Einsatz von Datenanalysen und KI in kritischer Infrastruktur

Die gegenseitige Abhängigkeit zwischen der Stromversorgung und der IKT wird ein zentrales Thema bleiben, vor allem in Bezug auf die Identifikation und Beherrschung von neuen kritischen Situationen bzw. kritischen Prozessen. Hierfür benötigt es klar definierte Strategien, um sowohl die Risiken zur Entstehung von Versorgungsausfällen zu minimieren als auch im Fehlerfall möglichst schnell das Netz zu stabilisieren. Das ganze Ausmaß möglicher Fehlerquellen, die die Digitalisierung und der Einsatz von KI mit sich bringen, ist bisher nicht eindeutig abzuschätzen. Durch die Veränderungen der Netzinfrastruktur im Zuge der Energiewende und Digitalisierung können weitere Risiken wie neuartige, komplexe Störereignisse hinzukommen.

Hinsichtlich der Datenabhängigkeit unterliegen KI-Systeme grundsätzlich den gleichen Schwachstellen wie andere traditionelle Methoden. Da KI-Anwendungen jedoch in der Regel größere Datenmengen und potenziell neue Datenquellen nutzen können, die von klassischen Methoden nicht verwendet werden, können KI-Methoden ein höheres Maß an Anfälligkeit für Datenfehler aufweisen. Daher muss darauf geachtet werden, dass die erhöhte Abhängigkeit von Daten mit einem hohen Maß an Genauigkeit und Zuverlässigkeit einhergeht. Hier bieten allerdings KI-Methoden selber die Möglichkeit, Daten im Vorfeld der Nutzung auf Validität und Konsistenz hin zu prüfen. Solche Schritte müssen aber auch umgesetzt und vorgeschaltet werden. KI-Methoden können auch so trainiert werden, dass sie fehlerhafte Daten oder feindliche Angriffe erkennen oder ihnen widerstehen können. Diese Maßnahmen sind jedoch nicht trivial in einer KI-Anwendung zu implementieren, daher muss diese Funktionalität neben dem primären Anwendungsfall selbst sorgfältig trainiert und bewertet werden.

Aktuell dienen die meisten Anwendungen, die Methoden der künstlichen Intelligenz nutzen, lediglich zur Verbesserung bestehender Prozesse. Optimierungsverfahren können Handlungsempfehlungen geben und bei der Entscheidungsfindung unterstützen, sie übernehmen aber nicht automatisiert den Netzbetrieb. Entscheidungen selbst liegen weiterhin bei dem systemverantwortlichen Personal.

Regulatorischer Rahmen

Die Datennutzung muss immer unter Beachtung des regulatorischen Rahmens erfolgen, speziell die Nutzung von personenbezogenen Daten unterliegt strengen Anforderungen der DSGVO. Ebenso spielt die Informationssicherheit in der Energiewirtschaft eine große Rolle, da die Inhalte in der Regel hoch sensibel sind und nur Zugriff für bestimmte Personenkreise gewährt werden darf.

Bei den meisten Anwendungen kann auf den Einsatz von personenbezogenen Daten verzichtet werden. Es existieren heute zahlreiche Verfahren, die mit aggregierten, anonymisierten Daten hinreichend genaue Ergebnisse liefern. Neben der Datenaggregation existieren zudem weitere spezielle Verfahren zur Anonymisierung, um die Nutzung von sensiblen Daten zu ermöglichen.

Die Nutzung von öffentlichen Datenquellen wird durch eine fehlende Open-Data-Mentalität in Deutschland erschwert. Die Regelungen hierzu unterscheiden sich je nach Bundesland.

Handlungsempfehlung: Freigabe nicht schützenswerter Daten

Daten, die nicht besonders schützenswert sind, sollten flächendeckend freigegeben werden (z.B. der Gebäudewärmebedarf). Nordrhein-Westfalen und Berlin nehmen hierbei eine Vorreiterrolle ein. Andere Bundesländer sollten dem Beispiel von NRW und Berlin folgen. Ein einheitliches System zum Datenabruf würde den Nutzen öffentlicher Datenquellen signifikant vereinfachen.

Eine der größten Herausforderung stellt die Ressourcenverfügbarkeit dar. Sowohl fehlt Personal mit entsprechendem Know-How, als auch die finanziellen Mittel dafür. Zudem fehlen weitgehend Anreize für die Netzbetreiber an einer qualitativ und quantitativ hohen Datengrundlage zu arbeiten und innovative Technologien einzuführen.

Handlungsempfehlung: Anreize schaffen

Klar definierte Vorgaben und Standards zur Datenvorhaltung/ Datenbereitstellung in Verbindung mit einer Kostenanerkennung könnten helfen die Datengrundlage flächendeckend hinsichtlich der Datenverfügbarkeit und Datenqualität zu verbessern. Als unterstützende Maßnahme, um die flächendeckende Integration von innovativen Anwendungen zu beschleunigen, sollten die Anreize erhöht werden. Hierbei sind gesetzliche Vorgaben und Unterstützungen denkbar, z.B. durch die Anreizregulierungsverordnung oder spezielle Förderprogramme für die Entwicklung neuartiger Methoden.

6.3 Abschließende Aussage und Bemerkung

Zusammenfassend kann man festhalten, dass der Einsatz von Anwendungen mit künstlicher Intelligenz zu keinem signifikant gesteigerten Risiko bei dessen Einsatz in kritischen Prozessen, bzw. Prozessen in kritischen Umfeldern führen muss. Wie in Kapitel 2 und speziell 2.2 beschrieben, besteht die größte Kritikalität in einem Ausfall von Prozessen, die für den Betrieb und die Einsatzfähigkeit der jeweiligen kritischen Infrastruktur unerlässlich sind. Hierzu wurden für den Bereich der Stromverteilernetze die Indikatoren

- Unmittelbare Auswirkungen des Prozesses
- Daten und Informationssicherheit
- Grenzwertverletzung mit Betriebsmittelgefahr sowie
- Prozessunterbrechung,

mit ihren Auswirkungen in den Bereichen

- Netzbetriebsführung und operative Planung
- IKT-Prozesse
- Instandhaltung sowie im
- Endkundenbereich

bewertet. Festzuhalten ist hier, dass die grundsätzlichen Risiken bereits durch die Verwendung und Abhängigkeit von Daten und datengetriebenen Prozessen herrühren. Fallen diese Prozesse aus, oder sind die Datengrundlagen unvollständig oder fehlerhaft, kann das zu massiven Problemen und Schäden im Netzbetrieb führen. Hierbei ist der Einfluss und somit die Kritikalität dieser datengetriebenen Prozesse umso stärker je näher der Prozess an der Echtzeit liegt oder je größer dessen Systemrelevanz ist. Methoden der künstlichen Intelligenz werden hierbei zu den datengetriebenen Prozessen gezählt und bilden darin teilweise zusätzliche Risiken. Diese Risiken und damit die Kritikalität des Einsatzes von KI-Anwendungen wurden in Kapitel 3 und speziell 3.3 beschrieben und können bei sorgfältiger Vorbereitung und Planung des Einsatzes der KI-Anwendungen minimiert werden. Hier stellt das größte Risiko der Mensch dar, der die Ergebnisse von KI-Anwendungen nicht mehr selber nachvollziehen kann und ihnen somit vertrauen muss. Ein übermäßig gesteigertes Vertrauen kann aber auch in neue Abhängigkeiten führen. Sensibilisierung und Bewusstmachung können hier Risiken minimieren.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] **Deutsche Energie-Agentur (dena) (2019)**: Künstliche Intelligenz für die integrierte Energiewende. Einordnung des technologischen Status quo sowie Strukturierung von Anwendungsfeldern in der Energiewirtschaft

[2] **Umweltbundesamt (2021)**: Energiebedingte Emmissionen. [Online] URL: https://www.umweltbundesamt.de/daten/energie/energiebedingte-emissionen#energiebedingte-treibhausgas-emissionen (abgerufen am 05.05.2022).

[3] **Bundesministerium für Wirtschaft und Klimaschutz (2022)**: Deutsche Klimaschutzpolitik. [Online] URL: https://www.bmwk.de/Redaktion/DE/Artikel/Industrie/klimaschutz-deutsche-klimaschutzpolitik.html (abgerufen am 05.05.2022).

[4] **Fraunhofer-Institut für System- und Innovationsforschung ISI, Consentec GmbH, ifeu – Institut für Energie- und Umweltforschung Heidelberg, Technische Universität Berlin (2021)**: Langfristszenarien für die Transformation des Energiesystems in Deutschland 3. Kurzbericht: 3 Hauptszenarien

[5] **Sozialdemokratische Partei Deutschlands (SPD), BÜNDNIS 90/DIE GRÜNEN, Freie Demokratische Partei (FDP) (2021)**: Koalitionsvertrag 2021-2025

[6] **Prognos, Öko-Institut, Wuppertal-Institut (2021)**: Klimaneutrales Deutschland 2045. Wie Deutschland seine Klimaziele schon vor 2050 erreichen kann. Zusammenfassung im Auftrag von Stiftung Klimaneutralität, Agora Energiewende und Agora Verkehrswende

[7] **50 Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, TransnetBW GmbH (2022)**: Szenariorahmen zum Netzentwicklungsplan Strom 2037 mit Ausblick 2045, Version 2023. Entwurf der Übertragungsnetzbetreiber. [Online] URL: https://www.netzentwicklungsplan.de/de/netzentwicklungsplaene/netzentwicklungsplan-20372045-2023

[8] **E-Bridge Consulting GmbH, Institut für Elektrische Anlagen und Energiewirtschaft (IAEW), RWTH Aachen, Oldenburger Institut für Informatik (OFFIS) (2014)**: „Moderne Verteilernetze für Deutschland“ (Verteilernetzstudie). Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

[9] **50 Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, TransnetBW GmbH**. Netzentwicklungsplan: NOVA-Prinzip. [Online] URL: https://www.netzentwicklungsplan.de/de/nova-prinzip (abgerufen am 05.05.2022)

[10] **Bundesnetzagentur (BNetzA) (2020)**: Höchstspannungs-Freileitungen. [Online] URL: https://www.netzausbau.de/N2000/DE/Technik/Freileitungen/freileitungen.html (abgerufen am 05.05.2022)

[11] **Deutsche Energie-Agentur (dena) (2020)**: Künstliche Intelligenz – vom Hype zur energiewirtschaftlichen Realität. Vertiefte Analyse von KI-Anwendungsfeldern in der Energiewirtschaft

[12] **H.-A. Krebs, P. Hagenweiler (2021)**: Innovationen und künstliche Intelligenz entlang der energiewirtschaftlichen Wertschöpfungskette unter Berücksichtigung der Datensicherheit und des Datenschutzes

[13] **Bundesverband der Energie- und Wasserwirtschaft (BDEW) (2020)**: BDEW-Branchenlösung Redispatch 2.0. Datenaustausch-, Bilanzierungs- und Abrechnungsprozesse

[14] **Umlaut energy GmbH (2021)**: Künstliche Intelligenz für das Stromnetz der Zukunft

[15] **Umweltbundesamt (2020)**: Netzausbau. [Online] URL: https://www.umweltbundesamt.de/themen/klima-energie/energieversorgung/netzausbau#Netzausbau (abgerufen am 05.05.2022)

[16] **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe**: Kritische Infrastrukturen. [Online] URL: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html;jsessionid=F1C36EEC68AEAC914323DEC3DAE7604F.live351 (abgerufen am 25.05.2022)

[17] **Mary Cummings (2004)**: Automation Bias in Intelligent Time Critical Decision Support Systems.

[18] **Raja Parasuraman, Dietrich Manzey (2010)**: Complacency and Bias in Human Use of Automation: An Attentional Integration. The Journal of the Human Factors and Ergonomics Society.

[19] **acatech – Deutsche Akademie der Technikwissenschaften e. V., Deutsche Akademie der Naturforscher Leopoldina e. V., Union der deutschen Akademien der Wissenschaften e. V. (2021)**: Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden?

[20] **TenneT TSO GmbH (2018)**: Freileitungsmonitoring, witterungsabhängiger Freileitungsbetrieb

[21] **Next Kraftwerke GmbH**: Was sind Kritische Infrastrukturen (KRITIS) in der Energiewirtschaft? [Online] URL: https://www.next-kraftwerke.de/wissen/kritis (abgerufen am 05.05.2022).

[22] **Bayerischer Rundfunk (2021)**: #Faktenfuchs: Kann ein Hackerangriff für einen Blackout sorgen? [Online] URL: https://www.br.de/nachrichten/deutschland-welt/faktenfuchs-kann-ein-hackerangriff-fuer-einen-blackout-sorgen,SbFarZE (abgerufen am 05.05.2022)

[23] **Bayerischer Rundfunk (2022)**: Ukraine vereitelt Cyberangriff auf Stromnetz. [Online] URL: https://www.br.de/nachrichten/deutschland-welt/ukraine-vereitelt-cyberangriff-auf-stromnetz,T2oWryH (abgerufen am 05.05.2022)

[24] **Deutsche Energie-Agentur (dena) (2018)**: Datenschutz und Datensicherheit. Status quo, Herausforderungen und Handlungsbedarf im Rahmen der Digitalisierung der Energiewirtschaft

[25] **IT Verlag für Informationstechnik GmbH (2020)**: Der Angriff auf das ukrainische Stromnetz schreibt Geschichte. [Online] URL: https://www.it-daily.net/it-

sicherheit/cybercrime/der-angriff-auf-das-ukrainische-stromnetz-schreibt-geschichte (abgerufen am 05.05.2022)

[26] **Zweites Deutsches Fernsehen (ZDF) (2019)**: Blackout - Angriff auf unser Stromnetz. [Online] URL: https://www.zdf.de/dokumentation/planet-e/planet-e-blackout---angriff-auf-unser-stromnetz-100.html (abgerufen am 05.05.2022)

[27] **Bundesnetzagentur (BNetzA) (2015)**: EU-Verordnung zur Festlegung einer Leitlinie für die Kapazitätsvergabe und das Engpassmanagement (CACM-Verordnung). [Online] URL: https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK06/BK6_86_int_Strom/862_cacm/cacm_node.html (abgerufen am 05.05.2022)

[28] **Bundesnetzagentur (BNetzA) (2015)**: IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz

[29] **ENTSO-E (2015)**: Common Information Model. [Online] URL: https://www.entsoe.eu/digital/cim/ (abgerufen am 05.05.2022)

[30] **E. Lambert (2011)**: CDPSM: Common distribution power system model: When, why, what, how, who? IEEE/PES Power Systems Conference and Exposition

[31] **Bundesnetzagentur (BNetzA) (2020)**: Vergabe von Frequenzen im Bereich 450 MHz. [Online] URL: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2020/20201116_450mhz.html (abgerufen am 05.05.2022)

[32] **50 Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, TransnetBW GmbH (2017)**. Generation and load data provision methodology - GLDPM. [Online] URL: https://www.netztransparenz.de/EU-Network-Codes/CACM-Verordnung/Generation-and-load-data-provision-methodology-GLDPM (abgerufen am 05.05.2022)

[33] **TransnetBW GmbH**: Redispatch 2.0. [Online] URL: https://www.transnetbw.de/de/strommarkt/systemdienstleistungen/redispatch-2-0 (abgerufen am 05.05.2022)

[34] **retoflow GmbH, Fraunhofer IEE, Institut für Energiewirtschaft und Energiesystemtechnik, Universität Kassel, Fachgebiet Energiemanagement und Betrieb elektrischer Netze (e²n)(2021):** Integration von operativer und strategischer Verteilnetzplanung durch eine modulare Datenplattform mit offenen Schnittstellen.

[35] **Deutsche Energie-Agentur (dena) (2018)**: Schnittstellen und Standards für die Digitalisierung der Energiewende. Übersicht, Status Quo und Handlungsbedarf

[36] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: Smart Meter Gateway. Dreh- und Angelpunkt des intelligenten Messsystems. [Online] URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/smart-meter-gateway_node.html (abgerufen am 05.05.2022)

[37] **Deutsche Energie-Agentur (dena) (2021)**: Digitale Marktkommunikation für das Energiesystem der Zukunft. Gutachten der umlaut SE inkl. Einordnung der dena

[38] **Presse- und Informationsamt der Bundesregierung (2021)**: E-Mobilität. Einfacher zahlen an der Ladesäule. [Online] URL: https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/novelle-ladesaeulenverordnung-1913026 (abgerufen am 05.06.2022)

[39] **Bitkom e. V., (2022)**: Bitkom zum Trilog der NIS-Richtlinie 2.0. Presseinformation. [Online] URL: https://www.bitkom.org/Presse/Presseinformation/Bitkom-zum-Trilog-der-NIS-Richtlinie-20 (abgerufen am 05.06.2022)

[40] **xmera Solutions GmbH**: IT-Sicherheitsgesetz Energieversorger & Neuregelung. [Online] URL: https://xmera.de/it-sicherheitsgesetz-energieversorger/ (abgerufen am 05.05.2022)

[41] **datenschutz.org (2022)**: Datensicherheit: Maßnahmen für den Schutz von Daten. [Online] URL: https://www.datenschutz.org/datensicherheit-massnahmen/ (abgerufen am 05.06.2022)

[42] **intersoft consulting services AG (2016)**: Unterschied zw. IT-Sicherheit, Datensicherheit, Datenschutz & Informationssicherheit. [Online] URL: https://www.dr-datenschutz.de/-unterschiede-zwischen-datenschutz-datensicherheit-informationssicherheit-oder-it-sicherheit/ (abgerufen am 05.06.2022)

[43] **DIN e.V., DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (2020)**: Deutsche Normungsroadmap Künstliche Intelligenz

[44] **Bitkom e. V., (2019):** Blick in die Blackbox - Nachvollziehbarkeit von KI-Algorithmen in der Praxis. [Online] URL: https://www.bitkom.org/sites/main/files/2019-10/20191016_blick-in-die-blackbox.pdf (abgerufen am 08.07.2022)

[45] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: IT-Grundschutz-Kompendium – 4. Auflage. [Online] URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI-/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=1 (abgerufen am 08.07.2022)

[46] **Z. Liu, N. Bornhorst, S. Wende-von Berg and M. Braun**, "A Grid Equivalent Based on Artificial Neural Networks in Power Systems with High Penetration of Distributed Generation with Reactive Power Control," NEIS 2020; Conference on Sustainable Energy Supply and Energy Storage Systems, 2020, pp. 1-7.

Abkürzungen

API	Application Programming Interface
ARegV	Anreizregulierungsverordnung
ASIDI	Average System Interruption Duration Index
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
CACM	Capacity Allocation and Congestion Management
CAPEX	Capital Expenditures
CDPSM	Common distribution power system model
CGMES	Common Grid Model Exchange Specification
CIM	Common Information Model
CPU	Central Processing Unit
dena	Deutsche Energie-Agentur
DSGVO	Datenschutzgrundverordnung
EE-Anlagen	Erneuerbare Energien-Anlagen
E-Kfz	Elektro-Kraftfahrzeug
ECMWF	Europäisches Zentrum für mittelfristige Wettervorhersage
EnWG	Energiewirtschaftsgesetz
ENTSO-E	European Network of Transmission System Operators for Electricity
EU	Europäische Union
GDEW	Gesetz zur Digitalisierung der Energiewende
GIS	Geoinformationssystem
GLDPM	Generation and Load Data Provision Methodology
GPU	Graphics Processing Unit
HiWi	Hilfswissenschaftler
HS	Hochspannung
HöS	Höchstspannung
IKT	Informations- und Kommunikationstechnik

IT	Informationstechnologie
IT-SiG	IT-Sicherheitsgesetz
IP	Internet Protocol
ISMS	Informations-Sicherheits-Maßnahmen-System
KNN	Künstliche Neuronale Netze
KI	Künstliche Intelligenz
KSG	Klimaschutzgesetz
KVS	Kabelverteilerschrank
ML	Machine Learning
MS	Mittelspannung
MsBG	Messstellenbetriebsgesetz
NABEG	Netzausbaubeschleunigungsgesetz
NN	Neuronale Netze
NIS	Netz- und Informationssicherheit
NRW	Nordrhein-Westfalen
NS	Niederspannung
ONS	Ortsnetzstation
OPEX	Operational Expenditures
OPF	Optimal Power Flow
PV	Photovoltaik
PwC	PricewaterhouseCoopers
REST	Representational State Transfer
RONT	Regelbarer Ortsnetztransformator
SCADA	Supervisory Control and Data Acquisition
SFTP	Secure File Transfer Protocol
SO GL	System Operation Guideline
StromNZV	Stromnetzzugangsverordnung
TOM	Technisch Organisatorische Maßnahme
ÜNB	Übertragungsnetzbetreiber
URL	Uniform Resource Locator
UW	Umspannwerk

VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
VNB	Verteilnetzbetreiber
WAFB	Witterungsabhängiger Freileitungsbetrieb