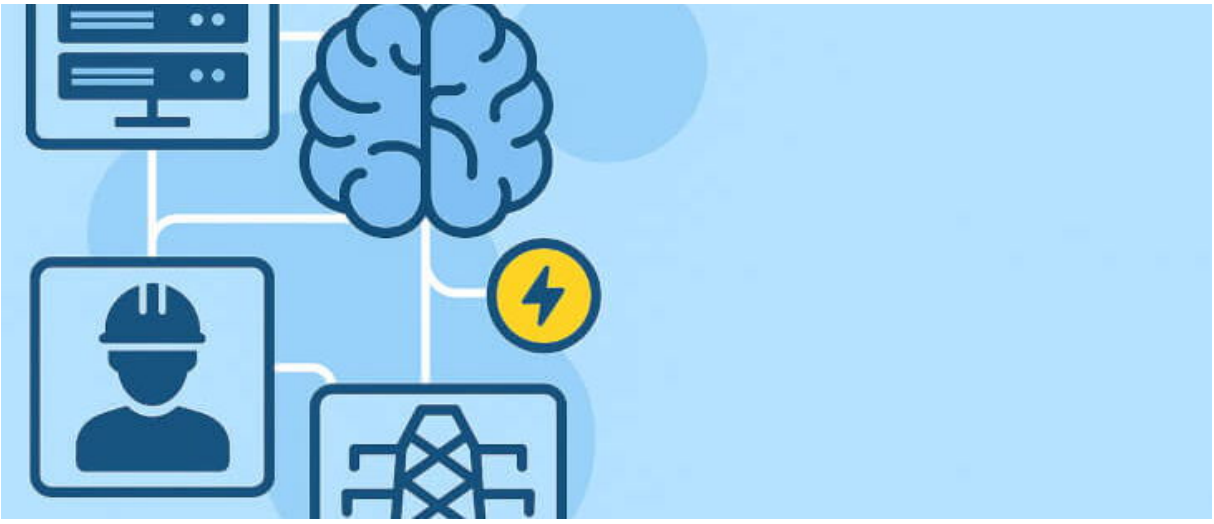
Künstliche Intelligenz im Stromnetz: Chancen, Risiken und neue Kompetenzen

27.10.2025, 10:18 Uhr
Kommentare: 0
Sicher arbeiten



KI-basierte Netzüberwachung wird in Rechenzentren unverzichtbar. © erstellt mit KI

Künstliche Intelligenz krempelt die Netzüberwachung in Rechenzentren grundlegend um: Plötzliche Lastspitzen, komplexe Wechselwirkungen und neue Anforderungen an die Sicherheit fordern Stromversorger und Elektrofachkräfte heraus. Wie lernende Systeme, Echtzeitdaten und adaptive Steuerung die Energieversorgung revolutionieren – und warum Fachkräfte jetzt mehr denn je zum Bindeglied zwischen Technik, IT und Regulierung werden.

Künstliche Intelligenz (KI) verändert die physikalische und organisatorische Struktur elektrischer Netze grundlegend. Rechenzentren, die bislang als stabile Großverbraucher galten, entwickeln sich zu dynamischen Systemen mit hochvolatilen Lastprofilen. Die enorme Rechenleistung moderner GPU-Cluster führt zu plötzlichen Leistungsanstiegen, die innerhalb weniger Sekunden mehrere Hundert Kilowatt betragen können. Diese Lastwechsel erzeugen transiente Spannungsverläufe, die Transformatoren und Schaltanlagen stark belasten. Besonders in Rechenzentren mit KI-Trainingssystemen treten solche Lastsprünge regelmäßig auf, wodurch Spannungseinbrüche und harmonische Verzerrungen zunehmen. Für Stromversorger ergibt sich daraus eine neue Form der Netzinstabilität, die herkömmliche Regelungsstrategien überfordert. Die Überwachung elektrischer Netze muss sich daher von statischen Messkonzepten zu lernfähigen, kontinuierlich analysierenden Systemen entwickeln.

Ein Rechenzentrum der neuesten Generation agiert als elektrischer Mikrokosmos. Jede Komponente beeinflusst die Spannungsqualität, jedes System kann eine Rückwirkung auf den Netzverlauf erzeugen. Hersteller wie Janitza beobachten in ihren Messreihen, dass in KI-Rechenzentren Oberschwingungen bis zur 35. Harmonischen auftreten. Diese Verzerrungen verändern das Leistungsfaktorverhalten, verursachen zusätzliche

Wärmeverluste und beeinträchtigen empfindliche Verbraucher. Die klassische Kompensation über starre Filter ist hier wirkungslos. Erst Echtzeitmessungen mit digital vernetzten Messgeräten erlauben es, die Netzzustände sekündlich zu erfassen und adaptive Kompensationsstrategien anzuwenden.

Spannungsqualität als Schlüsselparameter

Die Spannungsqualität bestimmt nicht nur die Effizienz, sondern auch die Lebensdauer der elektrischen Infrastruktur. In KI-Rechenzentren steigt der Anteil nicht linearer Lasten kontinuierlich. Leistungsfaktoren sinken, während Oberwellenströme den Neutralleiter stark beanspruchen. Hinzu kommen Rückwirkungen aus dynamischen USV-Systemen, die bei Lastumschaltungen kurzzeitig Blindleistung erzeugen. Um diesen Effekten zu begegnen, setzen Betreiber auf kontinuierliche Netzüberwachung nach EN 50160 „Merkmale der Spannung in öffentlichen Elektrizitätsversorgungsnetzen“ und ISO 50001 „Energiemanagementsysteme – Anforderungen mit Anleitung zur Anwendung“. Diese Normen fordern die Dokumentation der Netzqualität über lange Zeiträume, was nur durch automatisierte Analysesysteme realisierbar ist.

Aktuelle Energiemanagementsysteme erfassen Spannungsverlauf, Phasenwinkel, Frequenz und Oberschwingungen simultan. Die Daten werden über Cloud-Plattformen aggregiert, sodass Anomalien in Echtzeit erkannt und Maßnahmen ausgelöst werden können. Elektrofachkräfte müssen sich auf diese neuen Anforderungen einstellen, denn die Arbeit am Netz wird zunehmend datenbasiert. Die Fähigkeit, Messwerte zu interpretieren, ist nicht mehr ausreichend. Erforderlich ist das Verständnis, wie KI-Modelle Muster im Spannungsverlauf erkennen und daraus Handlungsempfehlungen ableiten.

Tipp der Redaktion



Elektrowissen zum Mitnehmen

- Lesen Sie spannende Expertenbeiträge.
- Stellen Sie unseren Fachexperten Ihre Fragen.
- Nutzen Sie die Download-Flat mit einer Vielzahl an Checklisten, Prüflisten, Arbeits- und Betriebsanweisungen.

Erste Ausgabe gratis!

Auch als Onlineversion erhältlich. Machen Sie mit beim Papiersparen.

KI-gestützte Netzsimulation und Systemanalyse

Das Forschungsprojekt GridAnalysis demonstriert die Verbindung von klassischer Elektrotechnik und maschinellem Lernen. Dabei wird die traditionelle Netzsimulation durch KI erweitert, um komplexe Wechselwirkungen zwischen Erzeugung, Verbrauch und Netzregelung abzubilden. Die Methode kombiniert stationäre Lastflussberechnungen mit neuronalen Netzen, die historische und synthetische Netzdaten analysieren. Durch diese Verbindung entsteht ein datengetriebenes Modell, das in Echtzeit neue Zustände bewertet. Die Simulation berücksichtigt dabei auch zufällige Ereignisse wie Schalthandlungen, Spannungseinbrüche oder das Auftreten von Kurzschlüssen.

In der Praxis wird eine große Zahl synthetischer Netzzustände erzeugt, die als Trainingsbasis dienen. Auf dieser Grundlage lernt das System, kritische Betriebszustände frühzeitig zu erkennen. Apache Kafka, Spark und TensorFlow ermöglichen es, Datenströme kontinuierlich auszuwerten und Vorhersagen zu generieren. So entsteht ein digitaler Zwilling des Netzes, der auf neue Belastungen reagiert, bevor diese im physikalischen System sichtbar werden. Für Elektrofachkräfte bedeutet das, dass Netzplanung und Betriebsführung künftig auf lernenden Modellen beruhen, die physikalische und statistische Methoden kombinieren.

Anomalieerkennung als Sicherheitsinstrument

Systeme wie PSIdetect erweitern die Überwachung um eine algorithmische Dimension. Sie vergleichen Soll- und Istzustände von Betriebsmitteln permanent und berechnen Anomalie-Scores, die Abweichungen vom normalen Verhalten kennzeichnen. Die Software wertet Messdaten aus Transformatoren, Schaltfeldern und Erzeugern aus und erkennt Muster, die auf Verschleiß, Überlast oder Manipulation hinweisen. Selbst geringfügige Abweichungen in Temperatur oder Schwingung werden identifiziert, bevor sie zu einer Störung führen.

Damit wird KI auch zur Voraussetzung für Netzsicherheit. Das IT-Sicherheitsgesetz verpflichtet Netzbetreiber zum Einsatz solcher Systeme. Sie müssen in der Lage sein, Anomalien in Echtzeit zu erkennen und geeignete Gegenmaßnahmen einzuleiten. Für Betreiber von Rechenzentren bedeutet das, dass die Grenzen zwischen IT-Sicherheit und elektrischer Sicherheit verschwimmen. Ein Angriff auf eine Regelkomponente kann dieselben Folgen haben wie ein technischer Defekt. Elektrofachkräfte müssen daher Systeme verstehen, die physikalische Anomalien ebenso analysieren wie digitale Angriffsversuche.

Veränderte Energieflüsse und Netzarchitekturen

Der steigende Energiebedarf durch KI-Workloads zwingt Versorger und Netzbetreiber, neue Strategien zu entwickeln. Prognosen gehen davon aus, dass der Energieverbrauch von Rechenzentren bis 2030 um bis zu 165 Prozent steigt. In den Vereinigten Staaten wächst der Anteil an der Gesamtstromnachfrage auf mehr als ein Zehntel. Diese Entwicklung betrifft auch Europa, wo die Netzplanung zunehmend auf die Verfügbarkeit erneuerbarer Energien ausgerichtet wird. Stromversorger müssen nicht nur für ausreichende Kapazität sorgen, sondern auch für Netzstabilität bei hoher Einspeisevolatilität.

McKinsey beschreibt die wachsende Abhängigkeit der Rechenzentrumsbranche von der Energieinfrastruktur. In vielen Regionen verzögern lange Vorlaufzeiten für

Transformatoren und Schaltanlagen den Ausbau neuer Standorte. Die Energieversorgung wird so zum Engpass der digitalen Infrastruktur. Investitionen in modulare Netzelemente und lokale Energiespeicher gewinnen an Bedeutung. KI kann hier helfen, indem sie Verbrauch und Einspeisung vorausschauend plant und Engpässe durch Lastverschiebung vermeidet.

Automatisierte Regelung und adaptive Steuerung

Das Zusammenspiel von Automatisierung und KI zeigt sich besonders in Projekten wie dem von WAGO und NTT Data entwickelten System zur energieoptimierten Rechenzentrumssteuerung. Dort überwachen Linux-basierte Steuerungen alle wesentlichen Aggregate und passen Betriebsparameter kontinuierlich an. Sensoren erfassen Temperatur, Luftstrom und Druck, während die Software die Daten in Echtzeit analysiert und die Regelkreise anpasst. Dadurch sinkt der Energieverbrauch der Kühlsysteme um bis zu 40 Prozent, ohne dass die Betriebssicherheit beeinträchtigt wird.

Diese Art der Selbstregelung verändert die Aufgaben in der Instandhaltung grundlegend. Wartung erfolgt nicht mehr nach festen Intervallen, sondern abhängig vom tatsächlichen Zustand der Anlagen. Die Verbindung von Messdaten, digitalem Zwilling und prädiktiver Analyse macht das Rechenzentrum zu einem autonomen System, das sich selbst überwacht. Für Elektrofachkräfte bedeutet das, dass Diagnose, Steuerung und Dokumentation zunehmend automatisiert erfolgen, aber stets fachlich überprüft werden müssen.

Downloadtipps der Redaktion

E-Book: Erstprüfungen nach DIN VDE 0100-600:2017-06

Hier gelangen Sie zum Download.

Checkliste: Prüfung der elektrischen Maschinenausrüstung – Einbauräume

Hier gelangen Sie zum Download.

Sichtprüfung von Maschinen nach VDE 0113-1 (Wiederholungsprüfung)

Hier gelangen Sie zum Download.

Checkliste: Energiemanagementsystem nach DIN VDE 0100-801

Hier gelangen Sie zum Download.

Vernetzte Sensorik und Edge-Analytik

Die nächste Stufe der Überwachung entsteht durch die Integration des Internet of Things (IoT). Sensoren für Temperatur, Feuchtigkeit, Stromstärke und Vibration liefern in hoher Frequenz Daten, die über Edge-Knoten ausgewertet werden. Diese lokale Vorverarbeitung reduziert den Datenverkehr und erhöht die Reaktionsgeschwindigkeit. IDC schätzt, dass drei Viertel aller Betriebsdaten künftig direkt am Netzrand verarbeitet werden. Die Kombination aus lokaler Rechenleistung und zentraler Analyse schafft ein zweistufiges System, das sowohl schnell als auch tiefgreifend reagiert.

Integrierte Plattformen wie die von etalytics verbinden diese Datenströme mit KI-Modellen,

die Energieflüsse in Echtzeit optimieren. Das Ziel ist nicht nur die Kostensenkung, sondern auch die Einhaltung ökologischer und regulatorischer Vorgaben. Systeme dieser Art werden bereits in Rechenzentren von Equinix eingesetzt, wo die Kühlenergie um fast die Hälfte reduziert werden konnte. Damit entsteht ein Beispiel, wie sich technische Effizienz und Nachhaltigkeit durch KI verbinden lassen.

Prädiktive Wartung und Netzresilienz

Die zustandsbasierte Wartung ersetzt heute schrittweise die reaktive Instandhaltung. KI-gestützte Systeme erkennen Muster, die auf bevorstehende Ausfälle hindeuten. Sie nutzen Schwingungsanalysen, thermische Signaturen und elektrische Kennwerte, um Verschleißprozesse frühzeitig zu identifizieren. Eine Studie der Internationalen Energieagentur zeigt, dass Unternehmen ihre Wartungskosten so um ein Fünftel senken können. Zusätzlich sinken ungeplante Ausfallzeiten erheblich, was die Verfügbarkeit kritischer Anlagen erhöht.

In Rechenzentren kommt hinzu, dass die Wartungsdaten direkt in das Energiemanagement einfließen. Das System passt seine Parameter automatisch an, um gefährdete Komponenten zu entlasten. Diese enge Verbindung von Überwachung, Steuerung und Wartung führt zu einer neuen Form betrieblicher Resilienz. Stromversorger profitieren von stabileren Lastprofilen, während Elektrofachkräfte Zugriff auf präzisere Diagnoseinformationen erhalten.

Lernende Systeme im Verteilnetz

Die Entwicklung geht über Rechenzentren hinaus. Projekte wie AI4Grids zeigen, dass auch Verteilnetzbetreiber künstliche Intelligenz einsetzen können, um Netzstabilität ohne kostspieligen Ausbau zu sichern. Im Pilotprojekt des Stadtwerks am See lernte ein KI-Regler aus realen Netzdaten, Spannung und Frequenz zu stabilisieren. Das System reagierte auf Lastspitzen durch temporäre Anpassungen und verhinderte so kritische Überlastungen. Die Ergebnisse zeigen, dass intelligente Regelung Lastmanagement, Einspeisung und Netzführung vereinen kann.

Gleichzeitig verdeutlichen Studien der VDE und der Deutschen Energie-Agentur, dass dafür sichere Datenräume notwendig sind. Offene Standards, semantische Interoperabilität und nachvollziehbare KI-Modelle werden zu Voraussetzungen für einen vertrauenswürdigen Netzbetrieb. Die Anforderungen des EU AI Act verstärken diesen Trend, indem sie Transparenz und Nachvollziehbarkeit in kritischen Infrastrukturen gesetzlich verankern.

Datenräume, Erklärbarkeit und Governance in der KI-Netzleittechnik

Die Einbindung von künstlicher Intelligenz in die Netzüberwachung verlangt nicht nur technische, sondern auch strukturelle und organisatorische Anpassungen. Die Studien der Deutschen Energie-Agentur und des VDE zeigen auch hier, dass der Erfolg von KI-Systemen in der Energietechnik maßgeblich von Datenverfügbarkeit, Interoperabilität und Erklärbarkeit abhängt. KI-Modelle können nur so präzise agieren, wie die ihnen zugrunde liegenden Daten es zulassen. Deshalb entstehen derzeit standardisierte Datenräume, die über Plattformen wie Gaia-X oder Data4Grid den Austausch zwischen Netzbetreibern, Herstellern und Forschungseinrichtungen ermöglichen. Diese Plattformen definieren

semantische Schnittstellen, die sicherstellen, dass Netz-, Betriebs- und Umweltdaten im gleichen Format verarbeitet werden können. So lassen sich Spannungsqualitätsdaten aus Rechenzentren mit Echtzeitmessungen aus Verteilnetzen zusammenführen. Nur durch diese Vereinheitlichung wird eine sektorübergreifende Netzintelligenz möglich, die Lastmanagement, Prognose und Schutztechnik integriert.

Die VDE-Studie hebt darüber hinaus hervor, dass erklärbare KI, sogenannte XAI, in der Netzleittechnik unverzichtbar wird. Entscheidungen eines neuronalen Netzes müssen für Ingenieure nachvollziehbar sein, um Vertrauen und Auditierbarkeit zu gewährleisten. Im Netzbetrieb heißt das, dass KI-Systeme ihre Entscheidungslogik offenlegen und dokumentieren müssen, z.B. wenn sie eine Umschaltung veranlassen oder Schutzparameter anpassen. Solche Systeme dürfen keine Blackbox bleiben, sondern müssen Teil eines nachvollziehbaren Regelungssystems sein. Das schließt die Integration mit bestehenden Schutzrelais, Leitsystemen und Fehlerschutzkonzepten ein. Besonders die Anbindung an Schutzsysteme in der Niederspannung erfordert hohe zeitliche Präzision und eine Absicherung gegen Fehlentscheidungen, da Fehltriggerungen unmittelbare Betriebsfolgen haben können.

Gleichzeitig zeigt McKinsey, dass die größten Fortschritte nicht allein durch neue Hardware oder Netzkapazität erzielt werden, sondern durch datenbasierte Effizienzgewinne. KI kann durch adaptive Prognosen und intelligente Steuerung die Netzreserven um bis zu 20 Prozent besser ausnutzen, was die Notwendigkeit physischen Netzausbaus reduziert. In Verbindung mit Simulationen aus dem Projekt GridAnalysis entsteht damit eine Perspektive, in der Netzplanung und Netzführung verschmelzen. Das Netz wird zum lernenden Organismus, der aus historischen Betriebsdaten Prognosen generiert, Entscheidungen simuliert und daraus Rückschlüsse auf reale Schalthandlungen zieht.

Der organisatorische Wandel ist ebenso bedeutend wie der technologische. Netzbetreiber müssen ihre Betriebsprozesse so umgestalten, dass KI-Systeme regelmäßig nachtrainiert, validiert und kalibriert werden. Dazu gehört die Festlegung von Datenqualitätsmetriken, die Sicherstellung der Nachvollziehbarkeit von Entscheidungen und die Schaffung von Fachrollen, die zwischen Elektrotechnik, Datenanalyse und Regulierung vermitteln. In der Praxis bedeutet das, dass Elektrofachkräfte künftig nicht nur Messwerte interpretieren, sondern auch die Zuverlässigkeit der zugrundeliegenden KI-Modelle prüfen. Diese Entwicklung führt zu einer neuen Form technischer Verantwortung, in der Mensch und Algorithmus gemeinsam die Netzstabilität sichern.

Neue Kompetenzfelder für Elektrofachkräfte im KI-Netzbetrieb

Die Einführung KI-basierter Netzüberwachung verändert das Berufsbild der Elektrofachkraft grundlegend. Während bisher die Analyse von Messwerten, die Durchführung von Schalthandlungen und die Instandhaltung im Vordergrund standen, rückt nun die Fähigkeit in den Mittelpunkt, mit datengetriebenen, lernenden Systemen zu arbeiten. Fachkräfte müssen die Funktionsweise von KI-gestützten Reglern verstehen, deren Eingangsgrößen interpretieren und deren Entscheidungen technisch bewerten können. Damit erweitert sich das Aufgabenspektrum um die Plausibilisierung algorithmischer Entscheidungen. Der Mensch bleibt dabei nicht Beobachter, sondern Sicherheitsinstanz, die zwischen physikalischem Verhalten und digitaler Modelllogik vermittelt.

Im praktischen Betrieb entsteht dadurch eine neue Arbeitsebene zwischen Netzleittechnik, Automatisierung und IT-Sicherheit. Elektrofachkräfte müssen in der Lage sein, zwischen

Netzparametern, Prozessdaten und Modellparametern zu unterscheiden. Sie übernehmen zunehmend die Aufgabe, Datenquellen zu validieren, Schnittstellen zu kontrollieren und Grenzwerte so zu konfigurieren, dass Fehlalarme und Fehltriggerungen ausgeschlossen werden. Diese Tätigkeit gewinnt an Bedeutung, da KI-Systeme zwar präzise Muster erkennen, aber auch fehleranfällig für Datenrauschen, Ausreißer oder fehlerhafte Sensordaten bleiben.

Das IT-Sicherheitsgesetz schreibt vor, dass Anomaliedetektionen in Leit- und Überwachungssystemen dokumentiert, nachvollziehbar und manipulationssicher betrieben werden. Damit wird die Elektrofachkraft zum Bindeglied zwischen technischer Infrastruktur und regulatorischer Nachweisführung. Sie muss Anomalien nicht nur erkennen, sondern auch deren Ursache und Eintrittswahrscheinlichkeit bewerten. Dies erfordert neben elektrotechnischem Wissen ein Verständnis für Datenverarbeitung, statistische Modelle und KI-Trainingsverfahren.

Auch organisatorisch verändert sich die Rolle. Fachkräfte agieren zunehmend in interdisziplinären Teams mit Data Scientists, Softwareingenieuren und Netzplanern. Sie übernehmen Verantwortung bei der Kalibrierung von KI-Systemen, definieren Trainingszyklen und prüfen die Konsistenz von Datenfeeds. Damit verschiebt sich der Schwerpunkt von der reaktiven Instandhaltung hin zur strategischen Systembetreuung. Die Sicherheit des Netzes hängt künftig auch von der Qualität der Datenerfassung, der Modellpflege und der menschlichen Überprüfung der automatisierten Entscheidungen ab.

Zukunftsperspektive für Stromversorger und Fachkräfte

Die Netzüberwachung der Zukunft vereint physikalische Präzision, datengetriebene Analyse und adaptive Steuerung in einem System. Rechenzentren entwickeln sich zu aktiven Teilnehmern des Energiesystems. Sie reagieren nicht nur auf Netzsignale, sondern liefern selbst Informationen zurück, die in die Regelung einfließen. Damit verschwimmt die Grenze zwischen Energieverbraucher und Netzkomponente.

Für Stromversorger entsteht die Aufgabe, diese Datenströme zu koordinieren und die Stabilität über immer komplexere Strukturen hinweg zu sichern. Für Elektrofachkräfte bedeutet dies eine Erweiterung ihres Kompetenzfelds. Sie müssen elektrische Anlagen ebenso verstehen wie KI-Modelle, Datenqualität ebenso beherrschen wie Schutztechnik. Die Zukunft der Netzüberwachung liegt in einem hybriden Wissen, das Elektrotechnik, Informatik und Systemtheorie verbindet.

KI ersetzt kein Fachwissen, sie verlangt es in höherer Präzision. Sie schafft die Grundlage für ein Netz, das sich selbst versteht und reguliert. In dieser neuen Infrastruktur hängt Stabilität nicht mehr allein von physikalischer Trägheit ab, sondern von der Fähigkeit des Systems, zu lernen und sich anzupassen. Damit beginnt für Energieversorger und Elektrofachkräfte eine Ära, in der Intelligenz nicht mehr nur in den Köpfen, sondern auch in den Netzen liegt.

Kurz und knapp

- KI-basierte Netzüberwachung wird in Rechenzentren unverzichtbar.
- Plötzliche Lastspitzen und komplexe Wechselwirkungen fordern neue Überwachungskonzepte.
- Echtzeitdaten und lernende Systeme ermöglichen adaptive Steuerung und frühzeitige Fehlererkennung.
- Elektrofachkräfte benötigen neue Kompetenzen im Umgang mit KI, Datenanalyse und IT-Sicherheit.
- Netzstabilität und Effizienz profitieren von prädiktiver Wartung und automatisierter Regelung.

Weitere Beiträge zum Thema

Einsatz von Künstlicher Intelligenz zur Fehlerdiagnose

Künstliche Intelligenz: neuer Schwung für die Energiewende

Smart Grids in kritischen Infrastrukturen

Lithium-Ionen-Batterien in Rechenzentren: Wartung und Umgang

Brandschutz für elektrische Installationen in Rechenzentren

Künstliche Intelligenz (KI)

Autor:

Thomas Joos

freiberuflicher Publizist



Thomas Joos ist freiberuflicher Publizist und veröffentlicht neben seinen Büchern auch Artikel für verschiedene Medien wie dpa, Computerwoche und C’t.

Seit seinem Studium der medizinischen Informatik berät er auch Unternehmen im Bereich IT, Security und Absicherung von Rechenzentren.