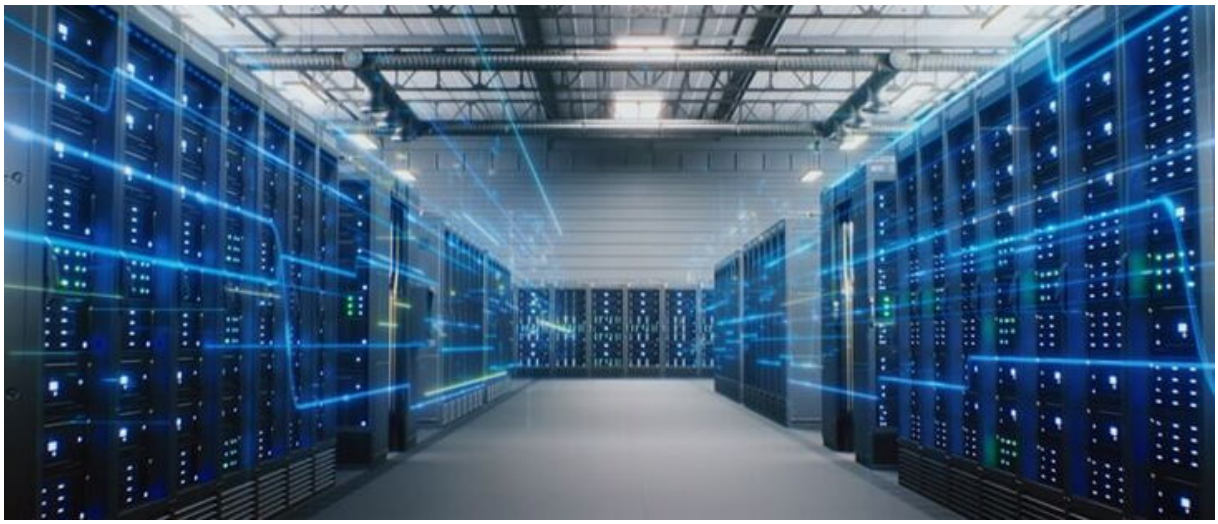
KI-basiertes Lastmanagement für USV-Systeme in Rechenzentren und Industrieanlagen (Teil 3)

06.03.2026, 14:00 Uhr
Kommentare: 0
Sicher arbeiten

Teil 3: KI-gestützte USV-Systeme – normative Anforderungen und Cybersecurity



KI-gestützte USV-Lösungen in Rechenzentren müssen normkonform, manipulationssicher und zuverlässig betrieben werden. © EvgeniyShkolenko/iStock/Getty Images Plus

KI-basiertes Lastmanagement macht USV-Anlagen zu intelligenten Energieknoten: Es senkt Lastspitzen, erhöht die Energieeffizienz, stabilisiert das Netz und schont Batterien sowie Komponenten. Gleichzeitig erfüllt es alle relevanten Normen und stärkt die Cybersecurity. So werden Rechenzentren und Industrieanlagen zuverlässiger, effizienter und zukunftssicher.

Teil 1: KI-basiertes Lastmanagement in USV-Systemen – Grundlagen und Funktionsweise

Teil 2: Intelligente Datenerfassung und prädiktive Steuerung im KI-basierten USV-Betrieb

Teil 3: KI-gestützte USV-Systeme – normative Anforderungen und Cybersecurity

Vorteile für Energieeffizienz durch KI

Im Bereich Energieeffizienz erlaubt KI eine optimale Nutzung der verfügbaren Energiequellen und Speicher. Durch Peak Shaving können Unternehmen Lastspitzen kappen, was in Ländern mit leistungsabhängigen Netzentgelten erhebliche Kosteneinsparungen bewirkt. Die KI verbessert hierbei die Effizienz, indem sie überschüssige Energie zu Nebenzeiten in die USV-Batterien lädt und zu Spitzenzeiten wieder abgibt. Dieses Vorgehen glättet die Leistungsaufnahme und verhindert teure

Lastspitzen, ohne die betrieblichen Abläufe zu beeinträchtigen.

Darüber hinaus trägt ein solches intelligent gesteuertes Energiemanagement zur besseren Auslastung von Ressourcen bei. Lasten werden möglichst in günstigere Tarifzeiten oder auf lokale Erzeugung (PV-Strom mittags) verschoben, was den Gesamtwirkungsgrad des Systems erhöht. KI-Lastmanagement kann auch externe Signale nutzen, z.B. Preissignale vom Energiemarkt (Demand Response), um dynamisch Verbraucher zu steuern. So wird Energie immer dann verbraucht, wenn sie am effizientesten bzw. günstigsten verfügbar ist. Das steigert die Energieeffizienz der Anlage insgesamt und unterstützt Unternehmen bei der Einhaltung von Energiezielen (ISO-50001-Energiemanagement oder gesetzliche Effizienzvorgaben). Nicht zuletzt ermöglicht die Künstliche Intelligenz eine engere Verzahnung mit erneuerbaren Energiequellen. Sie kann prognostizieren, wann Solaranlagen viel einspeisen, und diese Phasen aktiv nutzen, um Batterien zu laden oder Last vom Netz zu nehmen. Damit verbessert sich die Nutzung von Grünstrom, was Verbrauchern dabei hilft, die in vielen Ländern vorgeschriebenen Quoten für erneuerbare Versorgung einzuhalten.

Vorteile für die Netzstabilität

Hinsichtlich der Netzstabilität bietet KI-basiertes Lastmanagement ebenfalls Vorteile. Indem USV-Systeme nicht mehr nur als Verbraucher, sondern mit KI auch als stabilisierende Einspeiser agieren können, verschwimmen die Grenzen zwischen Verbraucher und Netzkomponente. Kritische Infrastrukturen wie Rechenzentren entwickeln sich so zu aktiven Teilnehmern im Stromnetz, die bei Bedarf Unterstützung liefern. Bei Engpässen können sie kurzfristig Last abwerfen oder sogar Energie aus den USV-Batterien ins Netz zurückspeisen, um Frequenz und Spannung zu stützen. Aus Netzsicht erhöht dies die Flexibilität. Die KI sorgt in diesem Kontext dafür, dass solche Eingriffe koordiniert und sicher erfolgen, z.B. dass die Einspeisung nur im Rahmen der Normen/Netzrückspeisebedingungen passiert und die Versorgung der eigenen Last trotzdem priorisiert bleibt.

Ein KI-optimiertes USV-System kann bei drohender regionaler Netzüberlastung frühzeitig seine Last reduzieren (Demand Response) und damit Schwarzstarts oder Lastabwürfe im Versorgungsnetz vermeiden. Die USV hält die Spannung für die eigenen Verbraucher trotz aller Schwankungen konstant, was die Betriebssicherheit erhöht. Frequenzschwankungen oder Flicker im Netz, wie sie bei hoher Einspeisung erneuerbarer Energien vorkommen, werden durch die KI-gestützte USV geregelt und erreichen die sensiblen Verbraucher gar nicht erst. Das macht die gesamte Stromversorgung robuster gegen äußere Einflüsse.

Downloadtipps der Redaktion

E-Book: „Industrie 4.0 in der Anwendung“

Hier gelangen Sie zum Download.

Unterweisung: Elektrofachkraft/verantwortliche Elektrofachkraft

Hier gelangen Sie zum Download.

Checkliste: Sichere Kabel- und Leitungsanlagen

Hier gelangen Sie zum Download.

Checkliste: Energiemanagmentsystem nach DIN VDE 0100-801

Hier gelangen Sie zum Download.

Lebensdauer der Komponenten

Ein oft unterschätzter Vorteil ist die Lebensdauer der Komponenten. Durch KI-Algorithmen wird die Beanspruchung von USV-Bauteilen und angeschlossenen Geräten erheblich reduziert. Elektronische Verbraucher profitieren davon, dass Spannungsspitzen und Transienten aktiv herausgefiltert werden; die KI hält die Versorgung sauber und innerhalb enger Toleranzen. Damit sinkt der Stress für Netzteile und Kondensatoren dieser Geräte, was deren Ausfallrate mindert. KI-gesteuertes Lastmanagement stabilisiert also nicht nur das Netz, sondern auch die Betriebselektrik im Werk oder Rechenzentrum, was zu weniger Störabschaltungen und längerer Haltbarkeit führt.

Insbesondere die USV selbst und ihre Batterien erfahren eine Lebensdauerverlängerung. Traditionell musste eine USV-Batterie bei jeder kleineren Netzstörung sofort reagieren, was zu häufigen Lade-/Entladezyklen führte. Mit KI-Optimierung wird dies minimiert, unerhebliche Fluktuationen werden vom Netzpuffer der USV (Kondensatoren oder Kurzzeitspeicher) abgefangen, ohne gleich die Batterie zu belasten. Die Batterie bleibt für echte Ausfälle voll verfügbar und wird im Normalfall innerhalb eines kontrollierten Ladefensters gehalten. Diese schonende Betriebsführung bewirkt, dass die Batterielebensdauer erhalten bleibt und seltener Ersatz beschafft werden muss.

Intelligente Lastverteilung für höhere Anlagenverfügbarkeit

Darüber hinaus verteilt KI die Last intelligent auf parallel geschaltete USV-Module (Stichwort: Lastbalancierung in redundanten N+1-Systemen), wodurch kein einzelnes Modul ständig am Limit läuft. Die thermische und elektrische Belastung wird gleichmäßiger, was Wartungskosten reduziert und ungeplante Ausfälle seltener macht. Summiert man diese Effekte, ergibt sich ein erhebliches Plus an Anlagenverfügbarkeit. Prozesse laufen störungsfreier, Wartungsintervalle können verlängert werden – und im Fehlerfall gibt es durch die vorausschauende Überwachung frühzeitig Warnsignale. Nicht zuletzt hilft KI auch, die Gesamtbetriebskosten zu senken. Neben den genannten Energieeinsparungen und Lebensdauergewinnen ergeben sich oft sekundäre Einsparungen. So kann die präventive Fehlererkennung über KI teure Folgeschäden vermeiden und der optimierte Betrieb der Kühlanlagen spart Stromkosten für die Klimatisierung ein.

Ein konkreter Nutzen ist auch, dass manche Förderprogramme oder regulatorische Vorteile genutzt werden können. Ein KI-gesteuertes Energiemanagement, das eine bestimmte Effizienzkennzahl verbessert, trägt dazu bei, neue gesetzliche Vorgaben zu erfüllen und Zuschüsse für innovative Energiesysteme zu erhalten.

Normative und regulatorische Anforderungen

Elektrotechnische Normen

IEC 62040-3 definiert die USV-Topologie-Klassifizierungen (VFI, VI, VFD) und Leistungskennzahlen; auch KI-unterstützte USV müssen nachweislich die entsprechenden Versorgungskategorien (VFI SS 111 für Online-USV) einhalten und die Umschaltzeiten und Spannungsgenauigkeiten liefern, die dort gefordert sind. Die Integration von KI entbindet nicht von der Erfüllung der einschlägigen technischen Normen. Vielmehr muss die KI innerhalb dieses normativen Rahmens arbeiten. Darüber hinaus gibt es branchen- und anwendungsspezifische Vorschriften, die den Einsatz von USV-Anlagen vorschreiben oder regeln, insbesondere in kritischen Infrastrukturen. So verlangt DIN VDE 0107 die Ausstattung medizinisch genutzter Bereiche mit Sicherheitsstromversorgung, sodass lebenswichtige Geräte bei Ausfall der Netzversorgung weiterbetrieben werden können.

KI-basierte USV-Steuerungen in solchen Umgebungen müssen also gewährleisten, dass die strikten Vorgaben erfüllt werden. Für Rechenzentren gibt die Norm EN 50600 klare Anforderungen an die Stromversorgungssicherheit vor, z.B. eine definierte Autonomiezeit durch USV und Notstromaggregate. Auch hier kann KI helfen, diese Vorgaben nicht nur zu erfüllen, sondern effizienter zu gestalten, z.B. durch optimale Dimensionierung der USV-Leistung. Für Industrieanlagen fordern die Betriebssicherheitsverordnung (BetrSichV) und verwandte Richtlinien, dass Anlagen bei Stromausfall kontrolliert heruntergefahren werden müssen.

KI-gestützte Lastmanagementsysteme könnten in solchen Fällen das geordnete Herunterfahren koordinieren und priorisieren, müssen aber vor allem fehlersicher sein, damit im Notfall nichts verzögert wird. DIN VDE 0833 und DIN EN 50171 schreiben in Bereichen der Sicherheitsbeleuchtung und Alarmanlagen eine zentrale Sicherheitsstromversorgung vor. Hier ist eher konservativer Betrieb gefragt (lange Überbrückungszeiten, hoher Zuverlässigkeitsfaktor), was eine KI-Steuerung aber durch Batterieoptimierung unterstützen kann. DIN EN 50272-2 regelt die Sicherheit von Batterien in Anlagen.

KI-Regularien und Sicherheitsanforderungen

Neben elektrotechnischen Normen treten zunehmend neue Regularien für KI-Systeme in Kraft. Der EU AI Act stellt eine gesetzliche Regulierung für den Einsatz künstlicher Intelligenz dar, die strenge Maßstäbe an KI in kritischen Infrastrukturen anlegt. Von KI-gesteuerten Netz- oder USV-Systemen wird gefordert, dass sie transparent, nachvollziehbar und sicher arbeiten. Betreiber müssen dokumentieren können, wie die KI entscheidet. Es müssen eingebaute Sicherungen gegen Fehlfunktionen vorhanden sein und die Modelle sollen möglichst erklärbar sein. Auch müssen entsprechende Risikobewertungen vorgenommen werden, bevor KI in sicherheitskritischen Bereichen eingesetzt wird. Deutschland hat bereits mit dem IT-Sicherheitsgesetz 2.0 vorgeschrieben, dass Betreiber kritischer Infrastrukturen Systeme zur Anomalieerkennung einführen müssen.

KI kann zwar Teil der Lösung sein, aber umgekehrt bedeutet es auch, dass eine KI-gestützte Steuerung als Teil der kritischen IT gesehen wird, die gegen Angriffe geschützt und behördlich nachweisbar manipulationssicher betrieben werden muss. Betreiber müssen also Vorkehrungen treffen, um die KI-Komponente gegen unbefugte Änderungen oder täuschende Eingaben abzusichern. Ferner spielen Standards wie ISO/IEC 27001 (Informationssicherheits-Management) oder IEC 62443 (IT-Sicherheit für industrielle Automatisierungssysteme) eine Rolle. Ein KI-Lastmanagement greift tief in die Steuerung der Stromversorgung ein und muss deshalb nach dem Stand der Technik gegen Cyberrisiken geschützt werden; entsprechende Managementprozesse und technische Maßnahmen sind oft Zertifizierungs- oder Gesetzesanforderung.

Schließlich sei erwähnt, dass Arbeitsschutz- und EMV-Richtlinien einzuhalten sind. So dürfen die eingesetzten KI-Steuergeräte keine unzulässigen elektromagnetischen Störungen verursachen und sollten, falls sie in Anlagen integriert werden, den Niederspannungsrichtlinien und CE-Kennzeichnungsanforderungen entsprechen.

Cybersecurity-Aspekte bei KI-gesteuerter USV-Steuerung

Die Verbindung von KI, Vernetzung und kritischer Stromversorgungsinfrastruktur macht das Thema Cybersecurity zu einem zentralen Aspekt. Wo früher eine USV weitgehend autonom und offline arbeitete, sind KI-basierte Lastmanagementsysteme typischerweise in Netzwerke eingebunden, sei es für Remote-Monitoring, für den Datenbezug oder für die Anbindung an Leitsysteme. Dadurch entsteht eine Angriffsfläche, die es abzusichern gilt. Ein erfolgreicher Cyberangriff auf die KI-Steuerung könnte im Worst Case ähnlich gravierende Auswirkungen haben wie ein technischer Defekt der Stromversorgung. So könnte ein Angreifer falsche Sensordaten einspeisen und die KI dazu bringen, die Batterie ungewollt zu entladen oder Lasten zur falschen Zeit abzuschalten. Um solchen Szenarien

vorzubeugen, müssen mehrere Ebenen der Sicherheit berücksichtigt werden:

- Die KI-Steuerung sollte in einem abgesicherten Netzsegment betrieben werden, getrennt von öffentlichen Netzen.
- Firewalls und Demilitarized Zones (DMZ) sorgen dafür, dass externe Zugriffe nur über definierte Schnittstellen und Protokolle möglich sind. Jede Fernkommunikation ist durch starke Authentifizierung und Verschlüsselung zu schützen.
- Prinzipiell ist der Zugriff strikt nach dem Prinzip der geringsten Rechte zu gestalten. Nur autorisierte Personen dürfen auf die Parameter der KI zugreifen – idealerweise durch ein mehrstufiges Berechtigungs- und Logging-System dokumentiert.
- Regelmäßige Sicherheitstests (Penetration Tests) sollten durchgeführt werden, um Schwachstellen im Setup frühzeitig zu erkennen.
- Da KI-Systeme in hohem Maße von der Korrektheit ihrer Eingangsdaten abhängen, muss die Integrität dieser Daten gewährleistet sein. Sensoren sollten manipulationsgeschützt installiert und gegen Sabotage gesichert sein.
- Außerdem kommen vermehrt Anomaliedetektionssysteme zum Einsatz, die ungewöhnliche Muster in den Steuerdaten erkennen. Interessanterweise kann hier wiederum KI helfen. Spezialisierte Algorithmen überwachen den Soll-Ist-Abgleich von Netz- und USV-Parametern und berechnen Anomalie-Scores. Weicht der Verlauf des Batteriestroms plötzlich vom üblichen Muster ab, was durch einen Cyberangriff verursacht sein könnte, würde ein solches System Alarm schlagen. In Deutschland sind Betreiber kritischer Infrastrukturen rechtlich verpflichtet, derartige Echtzeit-Anomalieerkennung einzusetzen und Abweichungen sofort zu melden bzw. Gegenmaßnahmen einzuleiten. Manipulationssicherheit bedeutet, dass die Modelle und Parameter gegen unautorisierte Änderung geschützt sind und dass Datenströme abgesichert übertragen werden.

Ein spezifischer Aspekt ist die Vertrauenswürdigkeit des KI-Modells selbst. Bei kritischen Anwendungen wird gefordert, dass KI-Systeme erklärbar und biasfrei sind, damit keine unerwarteten Entscheidungen getroffen werden. Betreiber müssen Verfahren etablieren, um die KI regelmäßig zu validieren und nachzutrainieren. Dazu gehört, Datenqualitätsmetriken festzulegen und kontinuierlich zu prüfen, ob die Sensordaten im erwarteten Rahmen liegen und ob das Modell darauf sinnvoll reagiert.

Im Kontext von Cybersecurity ist auch auf Adversarial Attacks zu achten. Theoretisch könnten Angreifer speziell präparierte Eingangsmuster ausnutzen, die die KI fehlleiten. Um dem zu begegnen, werden robuste Modellierungsverfahren genutzt und im Zweifel sicherheitskritische Pfade durch konventionelle Backups abgesichert.

KI-gestützte USV-Systeme machen deutlich, dass IT-Sicherheit und elektrische Sicherheit zusammen gedacht werden müssen. Elektrofachkräfte (EFKs) im Betrieb solcher Anlagen müssen ein Verständnis dafür entwickeln, dass ein Angriff auf digitale Steuerkomponenten die gleichen Konsequenzen haben kann wie eine physische Störung. Dementsprechend sind Notfallpläne zu erstellen, die auch Cybervorfälle einschließen. In solchen Fällen sollte die USV-Anlage auf einen sicheren Grundzustand zurückfallen, z.B. den rein statischen Doppelwandlerbetrieb ohne KI-Einfluss. Die Kompetenz der Mitarbeiter wird erweitert. Sie müssen lernen, die Ausgaben der KI kritisch zu hinterfragen und bei Bedarf manuell einzugreifen. Gleichzeitig ist es ihre Aufgabe, die Grenzwerte und Parameter der KI so zu konfigurieren, dass Fehlalarme minimiert werden und echte Angriffe dennoch erkannt werden.

Fazit

KI-basierte Lastmanagementsysteme transformieren USV-Anlagen von passiven Notstromgeräten zu intelligenten Energiezentralen. Sie ermöglichen es, Lasten dynamisch zu steuern, die Stromversorgung effizienter und stabiler zu machen und die Betriebsmittel zu schonen. Gerade vor dem Hintergrund steigender Leistungsdichten, z.B. durch KI-Workloads in Rechenzentren, und neuer Energieanforderungen bieten KI-gestützte USV-Systeme einen Weg, Zuverlässigkeit und Wirtschaftlichkeit in Einklang zu bringen. Für Elektrofachkräfte bedeutet dies, sich in neuen Feldern weiterzubilden – von der Datenanalyse über die IT-Sicherheit bis hin zur KI-Modellierung.

Die Technik entwickelt sich hin zu autonomen, selbstoptimierenden Stromversorgungssystemen, die dennoch dauerhaft unter menschlicher Aufsicht stehen müssen. Mit Beachtung der einschlägigen Normen und Sicherheitsaspekte kann KI im USV-Lastmanagement erhebliche Mehrwerte schaffen. Netzstabilität wird nicht mehr allein durch überdimensionierte Kapazitäten erreicht, sondern durch intelligente, lernfähige Steuerung, und Stromausfälle werden vom unberechenbaren Risiko zum beherrschbaren Szenario. Die KI liefert so einen Beitrag, dass kritische Infrastrukturen auch in Zukunft sicher und effizient mit Strom versorgt werden, selbst unter extremen Bedingungen.

Kurz und knapp

- Energieeffizienz: KI glättet Lastspitzen, optimiert Batterienutzung und verschiebt Lasten in günstige Tarifzeiten oder auf PV-Erzeugung.
- Ressourcennutzung: Dynamische Einbindung externer Signale wie Preissignale erhöht den Gesamtwirkungsgrad.
- Netzstabilität: USV-Anlagen werden zu aktiven Netzteilnehmern und können bei Bedarf Energie ins Netz zurückspeisen oder Last abwerfen.
- Längere Lebensdauer: Weniger Batteriezyklen, gleichmäßige Modulbelastung und gefilterte Spannungsspitzen reduzieren Verschleiß.
- KI-Systeme müssen u.a. DIN EN IEC 62040, EN 50600, DIN VDE 0107, DIN EN 50272-2 sowie EMV- und Sicherheitsanforderungen erfüllen.
- Cybersecurity: Geschützte Netzsegmente, starke Authentifizierung, Anomalieerkennung, manipulationssichere Sensorik und robuste KI-Modelle sind Pflicht.
- Bei Cyberangriffen oder Störungen muss die USV in einen sicheren Grundzustand wechseln können.
- Verbesserte Effizienzkennzahlen eröffnen Zugang zu Förderprogrammen und unterstützen die Erfüllung gesetzlicher Vorgaben.

Weitere Beiträge zum Thema

Künstliche Intelligenz (KI)

Künstliche Intelligenz: Neuer Schwung für die Energiewende

Predictive Maintenance in elektrischen Anlagen

Predictive Maintenance in der Energieverteilung: Wie künstliche Intelligenz Stromausfälle verhindern soll

Künstliche Intelligenz im Stromnetz: Chancen, Risiken und neue Kompetenzen

Einsatz von Künstlicher Intelligenz zur Fehlerdiagnose in elektrischen Anlagen

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.