Resilienz wichtiger als Reserven: KI als zentraler Faktor der Energieversorgung

Aktuelle Entwicklungen zeigen, dass Versorgungsstörungen nicht mehr ausschließlich auf technische Einzelereignisse zurückzuführen sind. Sie entstehen zunehmend aus dem Zusammenwirken systemischer Effekte wie steigenden Netzbelastungen, Volatilität, strukturellen Inkonsistenzen und gezielten Angriffen auf kritische Infrastrukturen. Damit verschiebt sich der Fokus von der Absicherung einzelner Komponenten hin zur Stabilität des Gesamtsystems.

Vor diesem Hintergrund gewinnt die Resilienz des Systems zunehmend an Bedeutung. Entscheidend ist die Fähigkeit, Störungen frühzeitig zu erkennen, betroffene Bereiche gezielt zu entkoppeln, Auswirkungen aktiv zu steuern und die Versorgung schnell wiederherzustellen. Versorgungssicherheit wird damit weniger durch die reine Verfügbarkeit von Reserven bestimmt als durch die Beherrschung komplexer Systemzusammenhänge und die Widerstandsfähigkeit gegenüber äußeren wie inneren Belastungen.

Eine wesentliche Voraussetzung hierfür ist die Fähigkeit des Energiesystems, flexibel auf veränderte Rahmenbedingungen und Störungen zu reagieren. Mit dem steigenden Anteil volatiler Erzeugung wird die Fähigkeit, Erzeugung, Verbrauch und Speicher kurzfristig auszubalancieren, zunehmend wichtiger als die reine installierte Leistung. Dafür sind Transparenz über Assets, Netzstrukturen und Topologien sowie eine umfassende Digitalisierung der Netze erforderlich. Insbesondere Mess-, Steuer- und Transparenzfähigkeit schaffen die Grundlage, verfügbare Flexibilitäten wirksam zu nutzen.

Mit der zunehmenden Digitalisierung und Vernetzung der Energiewirtschaft rückt zugleich die Cyberresilienz in den Mittelpunkt. Die enge Kopplung von IT- und OT-Systemen führt dazu, dass Cyberangriffe unmittelbare Auswirkungen auf den Netzbetrieb entfalten können. Versorgungssicherheit erfordert daher ein ganzheitliches Sicherheitsverständnis, das Prävention, Detektion, Reaktion und Wiederherstellung integriert. Informationssicherheit, Datenschutz und Governance müssen dabei in einem integrierten Managementansatz zusammengeführt werden, um eine durchgängige Schutz- und Reaktionsfähigkeit entlang der gesamten Wertschöpfungskette sicherzustellen.

Resilienz, Flexibilität und Cyberresilienz lassen sich künftig nur dann wirksam gewährleisten, wenn verfügbare Daten systematisch genutzt werden, um Entwicklungen frühzeitig zu erkennen und geeignete Maßnahmen rechtzeitig einzuleiten. Künstliche Intelligenz (KI) kann hierbei einen wesentlichen Beitrag leisten, indem sie Analysefähigkeit und Reaktionsgeschwindigkeit in zunehmend komplexen Energiesystemen erhöht. Voraussetzung sind qualitativ hochwertige Daten, klare Governance-Strukturen und sichere Systemarchitekturen. Unter diesen Bedingungen verbessert KI Prognosen, erhöht die Transparenz über den Netzzustand, unterstützt die Steuerung von Flexibilitäten und ermöglicht die frühzeitige Erkennung von Störungen. Dadurch lassen sich Entscheidungsprozesse beschleunigen und die Stabilität sowie Widerstandsfähigkeit der Energieversorgung nachhaltig stärken.

Handlungsseitig sind insbesondere der Ausbau von Flexibilitätsoptionen, die konsequente Digitalisierung der Netz- und Systeminfrastruktur sowie die Stärkung der Cyberresilienz erforderlich. Ergänzend bedarf es geeigneter regulatorischer Rahmenbedingungen für den sicheren und skalierbaren Einsatz von KI. Entscheidend ist ein ganzheitlicher Ansatz, der Infrastruktur, Daten, Technologie und Governance integriert. ■

Rui Manuel Faria Dinis

Head of Digital Business Consulting bei der Fichtner IT Consulting GmbH

Foto: Fichtner

© VDI Fachmedien GmbH & Co. KG, Düsseldorf 2026