Smart Grids in kritischen Infrastrukturen – Netzstabilität im Zeitalter von Extremwetter und Cybergefahren

06.06.2025, 07:58 Uhr
Kommentare: 0
Sicher arbeiten

Smart Grids gelten als Schlüsseltechnologie, um die Versorgungssicherheit aufrechtzuerhalten. (Bildquelle: kobpr2/iStock/Getty Images Plus)

Naturkatastrophen, volatile Energieerzeugung, Cyberangriffe und steigender Verbrauch stellen herkömmliche Netze zunehmend infrage. Smart Grids gelten als Schlüsseltechnologie, um Versorgungssicherheit unter verschärften Rahmenbedingungen aufrechtzuerhalten. Ihre Einführung markiert einen Paradigmenwechsel von starrer Stromverteilung hin zu einem lernfähigen, steuerbaren und widerstandsfähigen Versorgungssystem. Doch dabei gilt es einiges zu beachten.

Vom starren Netz zur intelligenten Struktur

Während das klassische Stromnetz auf zentrale Erzeugung ausgelegt war, verschiebt sich die Energieerzeugung heute durch Photovoltaik, Windkraft und Blockheizkraftwerke zunehmend in Richtung dezentraler Strukturen. Damit steigen auch die Anforderungen an die Verteilnetze, die nun bidirektionale Energieflüsse bewältigen müssen. Smart Grids erweitern das Netz durch digitale Kommunikation, automatisierte Steuerung und dezentrale Intelligenz. Sensorik und Aktorik liefern kontinuierlich Echtzeitdaten. Diese werden von zentralen und dezentralen Managementsystemen verarbeitet, um Lastflüsse zu optimieren, Spannungen zu stabilisieren und Fehlerzustände frühzeitig zu erkennen.

Der Einbau intelligenter Messsysteme ermöglicht eine granularere Beobachtung der Netzzustände. Smart Meter erfassen nicht nur den Verbrauch, sondern auch Netzparameter wie Spannung und Frequenz. Über SCADA- und EMS-Systeme werden die Daten an Leitstellen übertragen, wo bei Bedarf automatisierte Korrekturen eingeleitet werden. Systeme wie Phasor Measurement Units und Wide Area Monitoring ergänzen die

Steuerung um hochpräzise Zustandsanalysen, die vor allem bei dynamischen Lastwechseln und Störungen entscheidend sind.

Klimatische Extremereignisse als systemische Belastungsproben

Die zunehmende Häufung extremer Wetterlagen führt zu einer starken physischen Belastung der Netzinfrastruktur. Hurrikans, Hitzeperioden, Starkregen und Waldbrände zerstören Freileitungen, Transformatoren und Umspannwerke. In klassischen Netzen wirken solche Schäden wie ein Dominostein. Der Ausfall einzelner Komponenten kann zu Kaskadeneffekten führen, bei denen die Störungen überregionale Ausmaße annehmen. Smart Grids setzen diesem Szenario eine strukturierte Verteidigung entgegen. Durch automatisierte Fehlererkennung und lokale Isolation von Störquellen können Ausbreitungsketten durchbrochen werden. Im Idealfall gelingt es, Ausfälle auf einzelne Straßenzüge zu begrenzen, während über alternative Pfade weiterhin Strom zu kritischen Einrichtungen fließt.

Besondere Bedeutung kommt dabei sogenannten Mikrogrids zu. Diese Inselnetze umfassen lokale Erzeuger, Speicher und Verbraucher und können sich bei Netzausfall selbstständig vom Hauptnetz abkoppeln. In Tokio wurde diese Strategie nach den Katastrophen von 2011 gezielt umgesetzt. Mikrogrids sichern dort unter anderem Krankenhäuser und Evakuierungszentren gegen flächendeckende Stromausfälle. Ergänzt durch automatisierte Fehlersuche und selbstheilende Netzelemente ergibt sich eine deutlich höhere Ausfallsicherheit, selbst bei komplexen Krisenlagen.

Lernen von Tokio – adaptive Resilienz als Leitprinzip

Tokio hat mit dem Aufbau seines resilienten Energienetzes internationale Maßstäbe gesetzt. Die Einbindung dezentraler Strukturen, ergänzt durch Selbstheilungsmechanismen und automatische Steuerung, ermöglicht dort eine Versorgungssicherheit selbst unter katastrophalen Bedingungen. Kritische Infrastrukturen wie Kliniken oder Verkehrssteuerungen bleiben im Inselbetrieb funktionsfähig. Deutschland kann hiervon profitieren, indem es die Prinzipien auf seine eigene Netzstruktur überträgt. Besonders in ländlichen Regionen, wo Ausfallzeiten länger dauern, bieten mikrogridfähige Systeme in Verbindung mit Notstrom- und Speicherkapazitäten eine praktikable Lösung.

Cybersecurity als systemische Achillesferse

Mit der Digitalisierung des Stromnetzes geht eine wachsende Angriffsfläche einher. Jeder intelligente Zähler, jedes Übertragungsprotokoll, jede Schnittstelle erhöht die Anzahl potenzieller Eintrittspunkte für gezielte Manipulationen. Die Bedrohungslage reicht von klassischer Malware über Insider-Angriffe bis hin zu staatlich unterstützten Sabotageakten. Besonders problematisch sind sogenannte False Data Injection Attacks, bei denen manipulierte Messwerte gezielt in das Netz eingespeist werden. Diese führen zu falschen Netzentscheidungen, können Schutzsysteme auslösen oder ganze Netzbereiche destabilisieren. Noch kritischer wird es, wenn diese Angriffe unbemerkt bleiben, etwa weil sie den Prüfmechanismus zur Fehlererkennung gezielt umgehen.

In der Praxis zeigt sich, dass für kritische Infrastrukturen nicht dieselben Prioritäten gelten wie in der klassischen IT. Hier steht Verfügbarkeit an oberster Stelle. Erst danach folgen Integrität und Vertraulichkeit. Ein Krankenhaus ohne Strom ist handlungsunfähig, selbst wenn alle Daten sicher sind. Daher müssen Schutzstrategien für Smart Grids diesem Vorrang gerecht werden. Systeme zur Angriffserkennung sollten Angriffe nicht nur detektieren, sondern auch lokalisieren und im Idealfall rekonstruieren, um den Betrieb aufrechtzuerhalten.

Defensive Strategien und ihre Grenzen

Effektive Abwehrkonzepte im Smart Grid setzen auf gestufte Verteidigung. Prävention erfolgt über Verschlüsselung, Hardwaremodule und Redundanz bei kritischen Messstellen. Die nächste Ebene bildet die Detektion, häufig gestützt durch KI-Verfahren oder statistische Modelle. Bei erfolgreichem Angriff muss die Rekonstruktion falsifizierter Daten greifen, um Steuerungsbefehle weiter ausführen zu können. Ein vielversprechender Ansatz

ist die Moving Target Defense. Hier werden die Angriffsflächen regelmäßig verändert, etwa durch gezielte Änderung von Netzparametern. Angreifer, die ihre Attacke auf veralteten Topologien planen, scheitern an der veränderten Systemstruktur.

Doch auch dieser Ansatz hat Grenzen. Die Wirksamkeit hängt von der Systemstabilität, den wirtschaftlichen Kosten und der Integration dynamischer Elemente wie erneuerbarer Energien ab. Ein weiteres Problem ergibt sich bei maschinellem Lernen. Modelle, die auf statischen Netzstrukturen trainiert wurden, verlieren bei realen Ereignissen mit Linienausfällen oder Einspeiseschwankungen massiv an Genauigkeit. Die Herausforderung liegt darin, robuste, adaptive und interpretierbare Algorithmen zu entwickeln, die auch unter sich wandelnden Bedingungen zuverlässig arbeiten.

Resilienz durch Technik und Governance

Smart Grids bieten die strukturellen und technologischen Voraussetzungen, um kritische Infrastrukturen auch bei Krisen am Laufen zu halten. Doch Technik allein genügt nicht. Entscheidend ist, dass Regulierungsrahmen, Investitionsprogramme und Sicherheitsarchitekturen aufeinander abgestimmt sind. Kommunen, Betreiber und Versorgungsunternehmen müssen gemeinsam neue Konzepte für Netzresilienz umsetzen. Hierzu zählen

- die gezielte Förderung von Mikrogrids,
- der flächendeckende Smart-Meter-Rollout,
- standardisierte Cyberhärtung sowie
- klar definierte Verfahren zur Krisenkommunikation

im Falle eines großflächigen Ausfalls.

Der Umbau der Energieinfrastruktur ist damit nicht nur eine Frage technischer Innovation, sondern auch der systemischen Verantwortung. Wer Netzstabilität in Zeiten von Naturkatastrophen, geopolitischer Unsicherheit und wachsenden Angriffsflächen sichern will, kommt an Smart Grids nicht vorbei. Kritische Infrastrukturen müssen nicht nur versorgt, sondern geschützt, stabilisiert und flexibel gesteuert werden. Smart Grids schaffen dafür die Basis, wenn sie richtig umgesetzt und umfassend geschützt sind.

Weitere Beiträge zum Thema

KRITIS-Dachgesetz: Was auf Betreiber kritischer Infrastrukturen jetzt zukommt

Cybersicherheit: Herausforderung für kritische Infrastrukturen

Industrie 4.0 – Digitalisierung und Vernetzung

DIN VDE 0100-802: Das gilt für kombinierte Erzeugungs-/Verbrauchsanlagen (PEI)

Analyse von Cybersicherheitsbedrohungen in modernen elektrischen Steuerungssystemen

Smart Grid – Einsatz hoch entwickelter Stromversorgungssysteme

Basiswissen Cybersecurity – aktuelle Entwicklungen und Tipps

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.