

Positionspapier

Maßnahmen für die Erhöhung der Resilienz in den Stromnetzen als kritischer Infrastruktur

Verschiedene Vorfälle in der jüngeren Vergangenheit (zum Beispiel 2025: Blackout in Spanien, Januar 2026: Netzausfall im Berliner Süden nach Brandanschlag) unterstreichen die Notwendigkeit, die Energieversorgungsnetze resilient zu gestalten. **Die Versorgung muss auch bei unerwarteten technischen Ausfällen, physischen Angriffen auf Netzkomponenten, Cyberangriffen, Extremwetterereignissen, wie sie vermehrt im Zuge des Klimawandels auftreten, so weit wie möglich aufrechterhalten werden.** Zudem muss gewährleistet werden, dass sich das System nach einer Störung schnell erholen kann. Dies betrifft nicht nur die physischen Infrastrukturen, sondern auch die zur Steuerung und Messung eingesetzten Systeme, wie z.B. Telekommunikation.

Die klassischen Anforderungen an die Ausfallsicherheit der Stromversorgung betrachteten vor allem die Zuverlässigkeit der elektrotechnischen Systemkomponenten. Demnach kann der Betrieb bei Störungen oder bei Ausfall einer physischen elektrotechnischen Komponente durch die redundanten, weiterhin funktionsfähigen Komponenten ohne Unterbrechung weitergeführt werden. Für die Systemauslegung wurde dazu überwiegend das (N-1)-Kriterium angewandt. Künftig muss das immer komplexer werdende Stromversorgungssystem so angepasst werden, dass es die Ausbreitung von Störungen unterbindet oder zumindest deutlich reduziert und seine grundlegende Funktionsfähigkeit behält. Es muss Vorsorge dafür getroffen werden, dass sich das System nach Störungen schnell in einen akzeptablen Betrieb überführen lässt, sodass sich die Folgen auf ein Minimum beschränken („Safe-to-Fail“).



Aktuell werden verschiedene Handlungsoptionen diskutiert. Eine Zusammenarbeit dezentraler und zentraler Komponenten kann das Risiko kritischer Systemausfälle minimieren. Auch der verstärkte Einsatz großer Speicherkapazitäten kann einen deutlichen Beitrag zur Stabilität des Netzbetriebs sowie auch der Systemstabilität leisten, muss jedoch geeignet angereizt werden, zumal ein netz- wie systemdienlicher Betrieb nicht automatisch mit betriebswirtschaftlich optimierten Geschäftsmodellen von Betreibern einhergeht. Mit steigendem Anteil Umrichter gekoppelter Erzeugung und der damit einhergehenden Außerbetriebnahme konventioneller Kraftwerke sinken Rotationsenergie und Kurzschlussleistung. Neue Systemdienstleistungen müssen gezielt und in ausreichender Höhe bereitgestellt werden, damit Frequenz- und Spannungsstabilität erhalten bleiben. Für eine Erhöhung der Resilienz ist eine angemessene

Ersatzteilerhaltung sicherzustellen, um auftretende Störfälle schnell zu bewältigen und deren Auswirkungen in einem engen, zeitlich tolerierbaren Rahmen zu halten (Grafik: ZVEI 2026).

1 Im Folgenden verstehen wir unter resilientem Stromsystem:

„Resilientes Stromnetz: Stromversorgung bleibt auch bei massiven Störungen und unerwarteten Ereignissen – wenngleich mit temporär tolerierbaren Einschränkungen – prinzipiell verfügbar¹.“

¹ In Anlehnung an Definition: Projekt RESIST Fraunhofer, Folie 3.

Systemische Resilienz der Stromversorgung muss frühzeitig Berücksichtigung in der Planung und in **Netzbetriebskonzepten finden, sowie Redundanz kritischer physischer als auch informationstechnischer Komponenten, Systeme und Kommunikationsstrecken gewährleisten**. Je nach Potenzial der Auswirkungen können abgestufte Redundanzkonzepte ausreichend sein, bei denen Restrisiken trotz redundanter Auslegung verbleiben aber angemessen reduziert sind, gleichwohl aber wesentliche Funktionalität sicherstellen. Gewährleistung der Cybersicherheit bei der Digitalisierung ist essenziell, wirkt jedoch allein gegen den Einflussfaktor von Cybersecurity-Attacken und muss um physischen Schutz ergänzt werden. Dezentralisierung mit Microgrids können im Störfall kritische Lasten lokal und zeitlich begrenzt versorgen, wenn Inselbetrieb und Netzwiederaufbau technisch vorgesehen und regelmäßig erprobt sind.

Physische Resilienz erfordert auch im Verteilnetz eine Berücksichtigung des N-1 Konzepts analog zum Übertragungsnetz. Gleichwohl gilt für den gesamten Netzbereich, dass dieses rein auf primärtechnische Betriebsmittel angewandt zu kurz greift. Vielmehr müssen zudem auch sekundärtechnische Komponenten mit einbezogen sowie Abhängigkeiten durch räumliche Nähe der Betriebsmittel mitberücksichtigt werden. Weiterhin ist auch eine planbare Bereitstellung von Systemdienstleistungen für ein zunehmend Umrichter-dominiertes System dringlich geboten.

Entscheidend für die Auswirkung einer Störung, vor allem auf die Zeitdauer und Wiederherstellung des regulären Netzbetriebs ist dabei die Art des Einflussfaktors. Als wichtigste Einflussfaktoren mit Auswirkung auf das Stromsystem gelten:

- Exogene Gefährdungen (Naturkatastrophen, Extremwetterereignisse)
- Physische Anschläge (auf Netzbetriebsmittel und weitere Infrastrukturkomponenten)
- Cyberattacken (auf einzelne Komponenten, Betreiber oder aggregierte Anlagenverbünde)
- Zustand der Infrastruktur (z.B. Alter der Netzkomponenten und Peripherie)

Die Auswirkungen und Schutzmaßnahmen unterscheiden sich dabei grundsätzlich erheblich. Es können jedoch vorbereitend eine Reihe wirkungsvoller Maßnahmen getroffen werden. Von zentraler Bedeutung ist dabei, dass diese im kontinuierlichen, übergreifenden Risikomanagement der Netzbetreiber integriert werden.

2 Unsere Positionen

2.1 Kurzfristige Umsetzung (0-2 Jahre)

- Vulnerable Anschlussnehmer (z.B. Krankenhäuser, Rechenzentren, Wasserversorgung) werden priorisiert und für einen Inselbetrieb vorbereitet. Mindestanforderungen an Schutz und Regelung, Schaltbarkeit, Kommunikation und Betriebsprozesse werden festgelegt. Funktionstests und Übungen werden verbindlich eingeführt.
- Dezentrale Erzeuger, Batteriespeicher und steuerbare Lasten inkl. Wechselrichter werden für definierte Beiträge im Inselbetrieb qualifiziert. Betriebsgrenzen, Schutzparameter und Regelungsanforderungen werden einheitlich vorgegeben.
- Informationssicherheit für Leittechnik, Automatisierung und Kommunikation wird verbindlich umgesetzt und orientiert sich wo immer möglich an europäischer Gesetzgebung (CRA u.a.) sowie internationalen Normen (IEC 62443). Harmonisierte Sicherheitsprofile werden genutzt. Nationale Sonderwege und proprietäre Varianten werden vermieden. Zertifizierung nach international anerkannten Kriterien wie Common Criteria und EUCC genutzt, Schnittstellenvielfalt wird begrenzt.
- Betrieb im Störfall wird auch bei Teil-Ausfällen der IT und Kommunikation abgesichert. Nutzung von separaten Kommunikationsnetzen werden evaluiert und ermöglicht. Segmentierung, gesicherte Zugriffe, Protokollierung und Notfallprozesse werden umgesetzt und geübt.
- Physische Schwachstellen werden identifiziert und priorisiert beseitigt. N-1-Lücken sowie gemeinsame Trassen und gemeinsame Standorte werden bewertet. Ersatzteilhaltung, mobile Reservebetriebsmittel und Wiederherstellungsprozesse werden gestärkt.
- Die Digitalisierung der Ortsnetzstationen für die ins Auge gefassten Inselnetzbereiche ist zwingend erforderlich.
- Resilienz schwächende Änderungen bei laufenden Gesetzgebungsvorhaben werden vermieden (sog. Netzpaket, EEG-Novelle). Dezentralisierung muss als Stärke, nicht als Schwäche des System erkannt und ausgebaut und genutzt werden.
- Kurzfristige räumliche und zeitliche Verfügbarkeit für Netzkomponenten sind zu gewährleisten, dazu zählen auch einsatzbereite Netzersatzanlagen sowie Servicebereitschaft für die kurzfristige Aktivierung.

2.2 Mittelfristige Umsetzung (2-5 Jahre)

- Der flächendeckende Smart Meter-Rollout mit zertifizierten Smart Meter Gateways (SMGWs) inklusive realisierter Steuerungsfunktionalitäten verringert die Angriffsflächen für Cyberangriffe unbefugter Dritter auf dezentrale Anlagen < 10 kW, da sie höchste Sicherheitsanforderungen erfüllen, dezentral kaskadierbar sind. Von besonderer Bedeutung für die Gewährleistung der Resilienz sind steuerbare Anlagen.
- Microgrids werden zunehmend standardisiert skaliert und in die Betriebsführung integriert. Inselbildung, Synchronisierung, Wiederschaltung und Netzwiederaufbau werden reproduzierbar umgesetzt. Speicher werden technisch zur Aufrechterhaltung der Versorgungssicherheit (Schwarzstartfähigkeit) vorbereitet und eingesetzt. Informationssicherheit wird als Lebenszyklusanforderung umgesetzt. Beschaffung, Nachweisführung, Updatefähigkeit, sichere Fernwartung und Vulnerability-Management werden durchgängig geregelt. Die zellulären Energiesysteme können einen vergleichbaren Beitrag leisten.
- Notwendige Redundanzen werden in der Planung ganzheitlich betrachtet und ggf. als räumliche Trennung von kritischen Netzkomponenten umgesetzt. Zweite unabhängige Einspeisungen, ringförmige Strukturen und bedarfsgerechte Automatisierung werden umgesetzt. Gemeinsame Trassen und gemeinsame Standorte werden in der Redundanzbewertung explizit berücksichtigt. Korridortrennung, robuste Knoten, ausreichende Umschaltmöglichkeiten und regelbare Betriebsmittel werden im europäischen Übertragungsnetz realisiert.
- Systemdienstleistungen auf den unteren Spannungsebenen werden technisch spezifiziert, geprüft und planbar beschafft. Dazu zählen netzbildende Eigenschaften von Umrichtern, Spannungshaltung und Blindleistungsbereitstellung, schnelle Frequenzreserve, ausreichende Kurzschlussleistung am Netzknoten, Fehlerüberbrückungsfähigkeit, Schwarzstartfähigkeit und Netzwiederaufbauaufähigkeit.
- Stärkung von Konzepten für Netz-/Versorgungswiederaufbau: Nutzung etablierter Mess- und Steuerketten, dezentrale Steuerung von Teilnetzen kann helfen, analog zu §14a für Kleinanlagen. Erste gute Ansätze erkennbar, netzbildende Systeme stärken, auch mittels Digitalisierung und Dezentralisierung.
- Notstromversorgungszeiten für kritische Kommunikation werden auch bei längerem Netzausfall sichergestellt.
- Autarke, autonome Reaktion der Anlagen, z.B. bei der Einhaltung des Spannungsbandes als Anforderungen prüfen und ggf. in nächsten TAR-Überarbeitungen für Niederspannung aufnehmen, gleiches gilt für die Kommunikationsanbindung.
- Umsetzung von Austauschbarkeit und Interoperabilität aller Komponenten. Harmonisierung von Betriebsmitteln (sinnvoll für Lagerhalten und technischen sowie operativen Support) voranbringen. Unterstützung regionaler Lieferanten und Produktion für Kernkomponenten der Energietechnik, Ausbau der Produktionskapazitäten sowie Vorhalten von Service-/Wartungskapazitäten ermöglichen.

2.3 Langfristige Umsetzung (ab 5 Jahre)

- Dezentrale Resilienz wird zunehmend als Bestandteil der Netzarchitektur etabliert. Kritische Versorgungszellen erhalten definierte Mindestanforderungen an Überbrückungsdauer, Startfähigkeit und Wiederschaltung. Dabei ist darauf zu achten, dass innovative Lösungen angemessene Berücksichtigung finden können. Microgrids werden gezielt in die systemweiten Maßnahmen einbezogen.
- Digitale Architekturen werden für einen nachhaltigen Betrieb ausgelegt. Interoperabilität, Auditierbarkeit und international harmonisierte Sicherheitsanforderungen werden umgesetzt. Ein sicherer Mindestbetrieb im Störfall wird als Standardkonzept etabliert.
- Das Stabilitätsdesign für Netze wird weiterentwickelt, verbindlich verankert und umgesetzt, um einen zunehmenden Anteil netzbildender Umrichter verstärkt mit einzubeziehen. Netzanschlussregeln, Modellierung, Prüfverfahren und Schutzkoordination werden harmonisiert.
- Die grenzüberschreitende Vermaschung des europäischen Übertragungsnetzes wird ausgebaut, wodurch sich auch eine vorteilhafte Erweiterung der Leitungskapazitäten zwischen den Ländern ergibt.
- Der Ausbau dezentraler und verteilter Energieerzeugungsanlagen (PV und Wind) und Energiespeicher (BESS), wird auch zur Unterstützung bei regional und zeitlich begrenzten Ausfällen fortgeführt. Die lokale und regionale Vorhaltung von Reservekomponenten in Clustern, Sicherung der Lieferketten und Ausbau der Produktionskapazitäten, Stärkung von Energie-Ökosystemen werden gezielt unterstützt.

3 Zusammenfassung

- **Resilienz** im Stromnetz bedeutet Störungen zu verkraften, Auswirkungen zu begrenzen und Versorgung schnell wiederherzustellen.
- **Dezentralisierung** erhöht die lokale Handlungsfähigkeit und ermöglicht zeitlich begrenzte Überbrückung für kritische Lasten.
- **Digitalisierung** verbessert Transparenz und Steuerbarkeit, ist aber selbst kritische Infrastruktur und muss informationssicher betrieben werden.
- Generell ist zwischen Systemstabilität und lokaler wie regionaler Netzstabilität zu unterscheiden. Während Störungen in der Systemstabilität sich über nationale Grenzen hinweg, großflächig auswirken können sind, haben regionale oder lokale Störungen der Netzstabilität begrenzte und in der Regel gut beherrschbare Auswirkungen.
- **Physische Redundanz** bleibt Grundprinzip. Räumlich getrennte N-1-Redundanz reduziert Abhängigkeiten von einzelnen Betriebsmitteln, Standorten und Trassen.
- Zum **N-1-Prinzip**:
 - Das System ist so ausgelegt, dass in allen vorgesehenen Betriebsfällen jede Komponente ausfallen kann, ohne dass es zu einer Beeinträchtigung der Versorgung kommt.
 - N-1-Redundanz liegt vor, wenn zum Beispiel der Ausfall eines einzelnen relevanten Betriebsmittels durch eine Alternative kompensiert werden kann, die nicht auf derselben Trasse geführt wird und nicht am selben Standort konzentriert ist. Für die Bewertung sind Korridorrennung, unabhängige Einspeisepunkte, betriebliche Umschaltmöglichkeiten, Schutzkonzepte und verfügbare Systemdienstleistungen gemeinsam anzusetzen.



Wir unterstützen die Etablierung eines Resilienzdialogs zwischen allen relevanten Beteiligten, wie insbesondere Ministerien & Behörden, Regulierung, Netzbetreibern, Herstellern und Dienstleistern. Über die hier dargestellten Punkte hinaus sollten weitere Aspekte wie die Unterstützungsmöglichkeiten für kleinere Netzbetreiber in Form von Kooperationen oder die möglichen Wechselwirkungen verschiedener Regularien bearbeitet werden (Kohärenz herstellen und Widersprüche vermeiden). Für einen zielführenden Prozess sind eindeutige Zuständigkeiten und Ansprechpartner zwingend erforderlich.

Kontakt

Claudia Lorenz • Geschäftsführerin • Fachverband Energietechnik • Bereich Energie
Tel.: +49 30 306960-20 • Mobil: +49 162 2664-1518 • E-Mail: claudia.lorenz@zvei.org

ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Charlottenstr. 35/36 • 10117 Berlin
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 07.10.2026