

IZW FACHBEITRAG

INITIATIVE ZUKUNFT
WIRTSCHAFT DEUTSCHLAND E. V.

Millionen Anlagen. Immer mehr Leistung. Zu wenig Steuerbarkeit.

Deutschland im Blindflug.

Wie der rasante Ausbau dezentraler Erzeugungsanlagen die Steuerbarkeit des Stromsystems herausfordert – und was jetzt auf dem Spiel steht.

Autoren
Herbert Saurugg
Frank Oesterwind

IZW – INITIATIVE ZUKUNFT WIRTSCHAFT DEUTSCHLAND E. V.

Einstieg – physische Angriffe und der unsichtbare blinde Fleck

Anfang September wurde die deutsche Stromversorgung gleich mehrfach angegriffen. In Südbrandenburg verursachten Unbekannte mit selbstgebauten Flugkörpern Kurzschlüsse unweit des Umspannwerks Turnow-Preilack, was in Folge zu einem Kraftwerksausfall führte. Am selben Abend kam es zu einem ähnlichen Angriff am Umspannwerk Bergheim in Nordrhein-Westfalen, woraufhin fünf Braunkohleblöcke mit rund 3.000 Megawatt vom Netz genommen wurden. Die Ermittler sprechen von verfassungsfeindlicher Sabotage. Bereits im Januar und im tiefsten Winter hatte ein Brandanschlag auf eine Kabelbrücke in Berlin-Lichterfelde mehr als 40.000 Haushalte tagelang ohne Strom gelassen, den längsten Ausfall der Stadt seit 1945.

Das Netz hielt den Angriffen stand, weil das Übertragungsnetz nach dem n-1-Prinzip Reserven vorhält. Die Reaktion der Politik ist trotzdem vorhersehbar: Stacheldraht, Kameras, Drohnenabwehr, eine Verordnung zum Kritis-Dachgesetz. Das ist alles richtig – und es schützt genau eine Sorte von Anlagen: die, die man einzäunen kann. Die verwundbarste Stelle des künftigen Stromsystems steht dennoch nicht hinter einem Zaun. Sie hängt in Millionen Kellern und auf Millionen Dächern.

Versorgungssicherheit wird hierzulande vor allem als Mengenfrage verhandelt: genug gesicherte Leistung, genug Netze, genug Brennstoff. In einem System, das bis 2030 zu rund 80 Prozent erneuerbar sein soll, entscheidet jedoch eine weitere Größe: Beherrschbarkeit. Ende August überschritt die installierte Photovoltaikleistung 128 Gigawatt, verteilt auf mehr als sechs Millionen Anlagen; bis 2030 sollen es 215 Gigawatt sein. Dazu kommen Wärmepumpen, Wallboxen, Heimspeicher und Energiemanagementsysteme.

> **“ Millionen dezentrale Einzelkomponenten warten auf ihre Integration**

Wir bauen damit immer mehr dezentrale Einzelkomponenten zu. Daraus entsteht aber noch kein beherrschbares dezentrales Energiesystem. Ein System ist mehr als die Summe seiner Teile. Die entscheidende Frage lautet deshalb nicht, wie viele Geräte installiert wurden, sondern wie viel Erzeugungs- und Verbrauchsleistung tatsächlich sichtbar, erreichbar und regelbar ist.

> **“ Für die Versorgungssicherheit zählt nicht die Zahl installierter Geräte, sondern wie viele Megawatt das System tatsächlich sehen, erreichen und steuern kann.**

1. Messen ist nicht steuern – rund 50 Gigawatt im Blindflug

Ein intelligentes Messsystem misst und überträgt. Regeln kann es nichts. Dafür ist eine Steuerungseinrichtung nötig – im Messstellenbetriebsgesetz verankert, in der Praxis ein zusätzliches Gerät mit eigener Zertifizierung, Montage und eigenem Preis. In den meisten relevanten Anlagen ist diese Steuerungseinrichtung bislang nicht verbaut.

Zertifizierte Steuerungseinrichtungen gibt es erst in wenigen Produkten und Stückzahlen; zugleich fehlen industrielle Massenprozesse. Der Weg vom Netzsignal zum Gerät ist vielfach noch kein standardisierter Prozess:

Verbindungen müssen parametriert, getestet und über verschiedene Gewerke, Hersteller und Protokolle hinweg in Betrieb genommen werden. Was für Millionen Anlagen Routine sein müsste, ist vielfach ein Einzelfallprojekt geblieben.

> **Deutschland kann damit in Teilen Anlagen von 1985 schalten, aber nicht die von 2026.**

Entsprechend wird heute vor allem gesteuert, was die alte Welt ohnehin konnte: Nachtspeicherheizungen und ähnliche Bestandsanlagen, die seit Jahrzehnten über Rundsteuertechnik geschaltet werden. Kleine Photovoltaikanlagen, Wärmepumpen, Wallboxen und Heimspeicher – also genau jene Komponenten, die in Millionenstückzahlen hinzukommen – sind in der erforderlichen Breite nicht entsprechend steuerbar.

Nach fachlicher Abschätzung betrifft dieser blinde Fleck derzeit eine Größenordnung von rund 50 Gigawatt Erzeugungs- und Verbrauchsleistung. Zur Einordnung: Das entspricht größenordnungsmäßig der Leistung von etwa 50 großen Kraftwerksblöcken mit jeweils einem Gigawatt. Allerdings mit dem entscheidenden Unterschied, dass diese dezentrale Leistung nicht wie ein konventioneller Kraftwerkspark zentral sichtbar und regelbar ist.

> **Rund 50 Gigawatt im Blindflug: Der Ausbau skaliert – die tatsächliche Steuerbarkeit nicht.**

Der weitere Ausbau verschärft diese Diskrepanz: Die Photovoltaik soll von heute rund 128 auf 215 Gigawatt im Jahr 2030 wachsen; zugleich steigen die Stückzahlen von Speichern, Wärmepumpen und Wallboxen. Wenn die tatsächliche Steuerbarkeit nicht mindestens ebenso schnell wächst, wird der blinde Fleck größer statt kleiner.

Deutschland kann damit in Teilen Anlagen von 1985 schalten, aber nicht die von 2026. Politische Fortschrittsberichte, die primär Einbauquoten ausweisen, messen deshalb die falsche Größe. Die politische Zielgröße müsste erreichbare und regelbare Leistung sein.

2. Maximal sicher, minimal robust – wenn Gründlichkeit das Ziel unterläuft

Deutschland hat beim Smart-Meter-Gateway einen besonders anspruchsvollen Sicherheitsweg gewählt: Schutzprofile und Technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik, kryptografische Sicherheitsmodule und eine eigene Public-Key-Infrastruktur. Der hohe Sicherheitsanspruch ist grundsätzlich richtig.

Doch genau hier entsteht ein Paradox: Die Sicherheit einer einzelnen Komponente ist nicht automatisch die Resilienz des Gesamtsystems.

Der deutsche Sonderweg: eine Architektur aus einer anderen technologischen Zeit

Die Grundentscheidungen für die heutige deutsche Smart-Meter-Architektur reichen nach fachlicher Einordnung bis etwa 2013 zurück. Was nach Kalenderjahren überschaubar klingt, sind in der Digital-, Kommunikations- und

Halbleitertechnik technologische Epochen. Seitdem haben sich Leistungselektronik, Speicher, Photovoltaik, Elektromobilität, Cloud-Technologien und die Anforderungen an ein automatisiertes Stromsystem grundlegend weiterentwickelt.

Die deutsche Architektur wurde jedoch nicht von Grund auf für diese neue Systemwelt entwickelt. Stattdessen wurden über Jahre immer neue Anforderungen in das bestehende technische und regulatorische Grundkonzept integriert. Nicht jede alte Architektur lässt sich durch zusätzliche Funktionen unbegrenzt zukunftsfähig machen.

Deutschland geht dabei einen Sonderweg. Während international Messung und Kommunikation stärker voneinander getrennt sind und die Kommunikationseinheit im Kern die Funktion eines Modems übernimmt, wurden in Deutschland zusätzliche mess- und abrechnungsrelevante Funktionen in die Kommunikationsarchitektur integriert. Dadurch steigen Sicherheits- und Zertifizierungsanforderungen – zugleich werden Funktionen und Komponenten enger miteinander verkettet.

Wird ein zentraler Baustein verändert, ist deshalb nicht einfach ein Kommunikationsmodul auszutauschen. Die Änderung kann tief in eine zertifizierte Gesamtkette eingreifen und neue Qualifizierungs- und Zulassungsprozesse auslösen. Was ursprünglich ein besonders hohes Sicherheitsniveau gewährleisten sollte, kann damit ausgerechnet Austauschbarkeit, Innovationsgeschwindigkeit und Systemresilienz beeinträchtigen.

Der hohe deutsche Sicherheitsanspruch war und ist grundsätzlich richtig. Doch gerade die besonders komplexe Ausgestaltung kann inzwischen das ursprüngliche Ziel unterlaufen. Was einzelne Komponenten maximal absichern soll, erschwert zugleich ihre Austauschbarkeit, technologische Erneuerung und die Diversifizierung kritischer Lieferketten. So entsteht ein Sicherheitsparadox: Die Architektur erhöht die Sicherheit auf Komponentenebene – und kann gleichzeitig die Resilienz des Gesamtsystems schwächen.

> **„Die Sicherheit einer Komponente ist nicht die Resilienz eines Systems. Maximal sicher kann zugleich minimal robust bedeuten.**

Ein Fachmann brachte das Grundproblem im Gespräch bewusst drastisch und plakativ auf den Punkt: Über Jahre würden immer neue Anforderungen in eine bestehende Architektur integriert. Irgendwann könne auch ein Trabant nicht fliegen:

> **„Die deutsche Smart-Meter-Infrastruktur ist das perfekte Beispiel für den Versuch, einen „Trabanten“ so lange mit Zusatzmodulen zu überfrachten, bis er theoretisch fliegen müsste – was er in der Praxis aber nicht tut.**

Das Festhalten an der Architektur aus Smart-Meter-Gateway und separater, hochkomplex zertifizierter Steuereinheit hat eine technisch und regulatorisch sehr aufwendige Struktur entstehen lassen. Statt Millionen moderner Anlagen über standardisierte Massenprozesse einzubinden, bleibt die praktische Umsetzung vielfach komplex, hardwaregebunden und von „handwerklichen“ Einzelfallprozessen geprägt.

Eine rein inkrementelle Weiterentwicklung dieser Struktur greift zu kurz, da sie das Grundproblem nicht löst: Die Intelligenz wird in dedizierte, teure Hardware-Komponenten vor Ort gezwungen, während die moderne Tech-Welt längst softwarebasiert arbeitet.

3. Mehrere Hersteller, ein kritischer Chip – die unsichtbare Abhängigkeit

Zertifizierte Smart-Meter-Gateways werden von mehreren Herstellern angeboten. Das vermittelt zunächst den Eindruck einer diversifizierten Lieferlandschaft.

Bei einer sicherheitskritischen Kernkomponente besteht nach aktueller fachlicher Einordnung dennoch eine faktische Single-Source-Abhängigkeit, dem kryptografischen Sicherheitsmodul von NXP. Zwar existieren formal weitere zertifizierte Sicherheitsmodule. Entscheidend für die Resilienz ist jedoch nicht allein ein gültiges Zertifikat, sondern ob alternative Komponenten technisch aktuell, am Markt verfügbar und tatsächlich einsetzbar sind.

Mehrere Gateway-Hersteller bedeuten deshalb nicht automatisch mehrere unabhängige Lieferketten. Wenn alle Anbieter bei einem kritischen Baustein von derselben Quelle abhängen, entsteht hinter sichtbarer Produktvielfalt ein Single Point of Failure.

Eine Abkündigung, ein Lieferstopp oder ein Produktionsausfall träfe potenziell den gesamten weiteren Rollout. Ein Ersatzbauteil lässt sich wegen Neudesign, Requalifizierung und Zertifizierung nicht kurzfristig einsetzen; nach fachlicher Einschätzung und praktischer Erfahrung können entsprechende Prozesse mehrere Jahre beanspruchen – im ungünstigen Fall bis zu fünf Jahre.

Aus der Sicherheitsarchitektur kann so eine Abhängigkeitsarchitektur werden. Eine kritische Infrastruktur, die auf schwer ersetzbaren oder abgekündigten Komponenten ruht, ist kein Sicherheitsversprechen. Sie ist eine Hypothek.

> **“Aus der Sicherheitsarchitektur kann so eine Abhängigkeitsarchitektur werden.**

Auch wirtschaftlich hat die Konzentration Folgen: Wo nur ein kritischer Lieferant verbleibt, fehlt Wettbewerb. Zusätzlich müssen neben Chips auch Rohstoff-, Vorprodukt- und Cloud-Abhängigkeiten in die Resilienz Betrachtung einbezogen werden. Gleichzeitig kommunizieren viele Wechselrichter, Speicher und andere dezentrale Komponenten längst über Internetverbindungen und Hersteller-Clouds – mit einer Angriffsfläche, die mit jeder weiteren vernetzten Anlage wächst.

> **“ Mehrere Gerätehersteller schaffen keine Lieferkettenresilienz, wenn im Inneren alle vom selben kritischen Baustein abhängen.**

Der Sonderweg im internationalen Vergleich

Die meisten europäischen Nachbarländer sind beim Rollout deutlich weiter – ihre Architekturen gewichten Sicherheit, Standardisierung und Austauschbarkeit jedoch anders. Der deutsche Sonderweg muss sich deshalb nicht nur an seinem Anspruch, sondern an seiner tatsächlichen Systemwirkung messen lassen.

> **Ist man auf dem richtigen Weg, wenn alle anderen Geisterfahrer sind?**

Obwohl der Begriff „Smart Grids“ seit rund zwei Jahrzehnten verwendet wird, scheint das Thema für Deutschland in zentralen praktischen Fragen noch immer Neuland zu sein. Wenn ein System seinen Zweck – massentaugliche Sichtbarkeit und Steuerbarkeit – nicht erfüllen kann, muss auch der eingeschlagene Weg überprüft werden.

4. Die Rechnung zahlt die Allgemeinheit – auch ohne entsprechende Wirkung

Was sich netzseitig nicht unmittelbar steuern lässt, erfordert kostenintensive Ausgleichsmaßnahmen: Netzengpassmanagement, Reserveleistungen, Abregelungen oder zusätzlichen Netzausbau. Die Gesamtkosten für das Netzengpassmanagement beliefen sich im Jahr 2025 auf rund **3,08 Milliarden Euro**. Das betroffene Gesamtvolumen stagnierte auf einem hohen Niveau von rund **30.300 Gigawattstunden (GWh)**.

Die Detailstruktur der Kosten zeigt dabei die unterschiedlichen Hebel der Netzstabilitätsmaßnahmen auf:

- **1,18 Milliarden Euro** entfielen auf den klassischen Redispatch mit konventionellen Marktkraftwerken,
- **1,37 Milliarden Euro** wurden für die Vorhaltung und den Abruf von Reservekraftwerken aufgewendet,
- **435 Millionen Euro** flossen als finanzieller Ausgleich für abgeregelte Erneuerbare-Energien-Anlagen (EE-Anlagen), wobei die PV-Abregelung getrieben durch den starken Zubau um **94 Prozent auf rund 2.700 GWh** emporschnellte.

Besonders deutlich zeigt sich die Diskrepanz zwischen finanzieller Entlastung und tatsächlicher technischer Wirkung bei steuerbaren Verbrauchseinrichtungen (SteuVE) gemäß § 14a des Energiewirtschaftsgesetzes (EnWG). Betreiber von Anlagen wie Wärmepumpen oder Wallboxen erhalten eine Reduzierung der Netzentgelte, obgleich die für eine moderne, netzdienliche Steuerung erforderlichen intelligenten Messsysteme und Steuerboxen in der Praxis vielfach noch nicht flächendeckend installiert sind.

Gleichzeitig entstehen bereits beträchtliche Systemkosten für den Messstellenbetrieb und die regulatorisch geforderte Infrastruktur, die teilweise über die Netzentgelte auf die Gesamtheit der Stromkunden umgelegt werden. Somit werden Systemfunktionen refinanziert, deren tatsächlicher technischer Nutzen im Netzbetrieb zeitlich vorauseilt.

Auch die gesetzlichen Preisobergrenzen für intelligente Messsysteme wurden im Zuge regulatorischer Anpassungen angehoben, obwohl der vollständige flächendeckende Steuerungseffekt noch aussteht – ein Umstand, der im Folgenden anhand der Novelle des Messstellenbetriebsgesetzes (MsbG) vom Februar 2025 sowie einer Gegenüberstellung der bis dato gültigen Alt- und der neuen Obergrenzwerte systematisch belegt wird.

> **Bezahlt wird die Bereitschaft zur Steuerung. Entscheidend wäre aber die tatsächlich steuerbare Leistung.**

5. Was jetzt zu entscheiden ist

Unter Druck stehen damit alle drei Ziele der Energiepolitik zugleich: die Versorgungssicherheit, weil relevante Leistung nicht ausreichend regelbar ist; die Wirtschaftlichkeit, weil fehlende Steuerbarkeit und technologische Lock-ins Systemkosten erzeugen; und die Klimaverträglichkeit, weil ein System ohne ausreichende Beherrschbarkeit zusätzliche volatile Erzeugung nur mit wachsenden Ausgleichs- und Netzkosten integrieren kann.

Den Takt gibt der weitere Zubau vor. Bis 2030 wachsen Photovoltaik, Wind, Wärmepumpen, Elektromobilität und Speicher parallel. Ein massentauglicher Steuerungsrollout, der erst gegen Ende des Jahrzehnts funktioniert, kommt für einen erheblichen Teil des bis dahin aufgebauten Systems zu spät.

Die Frage lautet deshalb nicht mehr nur, ob die deutsche Architektur auf dem Papier sicher ist. Sie lautet, ob sie rechtzeitig verfügbar, massentauglich, tatsächlich steuerbar, technologisch aktualisierbar und im Fehlerfall ersetzbar ist.

Eine künftige Architektur muss Messung und Steuerung funktional zusammen denken, industrielle Massenprozesse ermöglichen, belastbare und möglichst offene Schnittstellen schaffen, mehrere qualifizierte Lieferquellen zulassen, kritische Single Points of Failure vermeiden und technologische Erneuerung ermöglichen.

Welche konkrete Systemarchitektur diese Anforderungen am besten erfüllt, wird in diesem Beitrag bewusst offengelassen. Nach dem vertiefenden Fachgespräch hat sich gezeigt, dass zunächst die vorgelagerte Botschaft erklärt werden muss: Die heute ausgerollte Mess- und Steuerungsarchitektur erfüllt wesentliche Voraussetzungen für die Beherrschung des immer komplexeren Stromsystems selbst noch nicht. Der „Blindflug“ ist damit das erste Problem, das sichtbar gemacht werden muss.

> **“ Wie viel Blindflug wollen wir uns noch leisten, wenn wir gleichzeitig über Resilienz, Souveränität und Versorgungssicherheit sprechen?**

Fazit – Zeit zur Wende

Deutschland elektrifiziert Wirtschaft und Industrie sowie Wärme und Mobilität. Damit wächst die Abhängigkeit von einem Stromsystem, das nicht nur genügend Energie bereitstellen, sondern Millionen dezentrale Einzelkomponenten in Echtzeit beherrschen muss. Der physische Ausbau läuft schnell. Die digitale und steuerungstechnische Beherrschbarkeit hält bislang nicht Schritt.

Die deutsche Energiewende sollte eine Blaupause für die Welt sein. Eine Voraussetzung dafür ist jedoch eine digitale und steuerungstechnische Infrastruktur, die massentauglich, zukunftsfähig und resilient ist. Genau daran bestehen erhebliche Zweifel: Die Grundarchitektur reicht in eine andere technologische Zeit zurück, der deutsche Sonderweg erschwert technologische Erneuerung, kritische Komponenten schaffen neue Abhängigkeiten und die Zahl installierter Geräte sagt noch wenig über tatsächlich steuerbare Leistung aus.

Der deutsche Sicherheitsanspruch ist richtig. Doch Sicherheit darf nicht an der einzelnen Komponente enden. Wenn hohe Zertifizierungshürden technologische Erneuerung erschweren, wenn mehrere Gerätehersteller an derselben kritischen Komponente hängen und wenn installierte Messsysteme mit tatsächlicher Steuerbarkeit verwechselt werden, kann das ursprünglich gut gemeinte Sicherheitskonzept sein eigenes Ziel teilweise unterlaufen.

Der Maßstab für Fortschritt muss sich deshalb ändern: weg von installierten Stückzahlen, hin zu tatsächlich sichtbarer, erreichbarer und regelbarer Leistung. Smart Meter sind kein Selbstzweck. Entscheidend ist, ob das Gesamtsystem seinen Zweck erfüllt.

Die Energiewende ist kein einmaliges Projekt, sondern eine Daueraufgabe. Technische und regulatorische Grundentscheidungen müssen deshalb überprüfbar und korrigierbar bleiben, wenn sich Anforderungen und Technologien grundlegend verändern. Zeit zur Wende, bevor der deutsche Weg der Energiewende an seiner eigenen Komplexität scheitert.

QUELLEN & AUTOREN

Gesetzestexte, Rahmendaten und Quellen

Regulatorischer Rahmen zur Digitalisierung (Smart Metering)

- **Messstellenbetriebsgesetz (MsbG)**: Regelt die gesetzlichen Grundlagen des Smart-Meter-Rollouts und die technische Trennung von intelligenten Messsystemen und Steuerungseinrichtungen.
- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**: Veröffentlicht die Technischen Richtlinien (BSI TR-03109) und Schutzprofile zur Cyber-Sicherheit der Gateways.
- **VDE FNN (Forum Netztechnik/Netzbetrieb)**: Definiert die technischen Anwendungsregeln für die digitale Steuerung und Parametrierung dezentraler Erzeugungsanlagen.

Energiewirtschaftliche Rahmendaten & Netzbetrieb

- **Bundesnetzagentur (BNetzA) – Marktstammdatenregister**: Dient als Primärquelle zur Überprüfung der installierten Photovoltaikleistung und der Gesamtzahl dezentraler Anlagen in Deutschland.
- **Übertragungsnetzbetreiber (50Hertz / Amprion)**: Liefern technische Berichte zum n-1-Prinzip, den Systemstabilitäts-Reserven und den Lastflüssen während der Netzstörungen.
- **Erneuerbare-Energien-Gesetz (EEG)**: Verifiziert die gesetzlichen Ausbauziele der Bundesregierung für das Jahr 2030, insbesondere die Zielgröße von 215 Gigawatt Solarleistung.
- **Bundesverband der Energie- und Wasserwirtschaft (BDEW)**: Bietet Fachpublikationen zur Netzintegration von dezentralen Großverbrauchern wie Wärmepumpen und Speichern.

Quellen:

- Smart-Meter-Gateway / Sicherheitsarchitektur / Sicherheitsmodul, BSI: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Sicherheitsmodul/sicherheitsmodul_node.html
- Gesetz zur Digitalisierung der Energiewende / Messstellenbetriebsgesetz – Gesetzgebungsverfahren und regulatorischer Rahmen, Deutscher Bundestag, Bundestag: https://dserver.bundestag.de/brd/2015/0543-15.pdf
- Kosten des Netzengpassmanagements 2025, Bundestag-Bericht zu den Netzengpasskosten: https://www.bundestag.de/presse/hib/kurzmeldungen-1210750
- Kosten des Netzengpassmanagements 2025, Bundesnetzagentur / SMARD: https://www.smard.de/page/home/topic-article/444/219906/massnahmenvolumen-im-gesamtjahr-stabil
- Gesetz für den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen, BSI: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/Smart-Metering-GDEW-MsbG/smart-metering-gdew-msbg_node.html
- Übersicht über zentrale Inhalte der Novelle des Messstellenbetriebsgesetzes 2025, VKU: https://www.vku.de/themen/infrastruktur-und-dienstleistungen/artikel/uebersicht-ueber-zentrale-inhalte-der-novelle-des-messstellenbetriebsgesetzes-2025/
- Rechtsgrundlage und Mechanismus § 14a EnWG, Vorgaben zu steuerbaren Verbrauchseinrichtungen, der garantierten Mindestleistung von 4,2 kW und den Modulen zur Netzentgeltreduzierung, Bundesnetzagentur: https://www.bundesnetzagentur.de/DE/Vportal/Energie/SteuerbareVBE/start.html
- Netzengpassmanagement im Q4 und Gesamtjahr 2025, Bundesnetzagentur, SMARD: https://www.smard.de/page/home/topic-article/444/219906/massnahmenvolumen-im-gesamtjahr-stabil
- Redispatch, Kosten, BWE: https://www.wind-energie.de/fileadmin/redaktion/dokumente/publikationen-oeffentlich/themen/04-politische-arbeit/01-gesetzgebung/20260421_Faktencheck_Redispatch.pdf
- Solarstrom-Abregelung steigt um 97 Prozent – Redispatch-Zahlen 2025 veröffentlicht, ZfK: https://www.zfk.de/energie/strom/redispatch-2025-pv-abregelung-verteilnetz

Autoren

Herbert Saurugg



Herbert Saurugg ist ein international anerkannter Experte für Blackout- und Krisenvorsorge sowie ehemaliger Berufsoffizier des österreichischen Bundesheeres im Bereich Cybersicherheit. Seit 15 Jahren beschäftigt er sich mit den systemischen Veränderungen und Zusammenhängen im europäischen Stromverbundsystem und warnt regelmäßig davor, die steigende Komplexität und deren Folgen nicht zu unterschätzen.

www.saurugg.net

Frank Oesterwind



Frank Oesterwind ist seit 2010 und mit Gründung der enerson Unternehmensgruppe unternehmerisch und Unternehmensberater in der Energiewirtschaft und im Mittelstand tätig. Zuvor war er ab 1990 als Führungskraft (C-Level) in der Ruhrgas AG, im E.ON und RWE-Konzern für die IT, Vertriebsaktivitäten und Shared Services verantwortlich.

Oesterwind ist Diplom-Kaufmann und hat Wirtschaftswissenschaften mit den Schwerpunkten Informatik, Organisation und Unternehmenssteuerung studiert.

LinkedIn: Frank Oesterwind

Herausgeber

IZW – Initiative Zukunft Wirtschaft Deutschland e. V.

Stand:

September 2026

Bildnachweise

Titelbild / KI-Illustration: KI-generiert mit ChatGPT/OpenAI, 2026.

Foto Herbert Saurugg: Business Foto Wien.