# Infrastruktur der Wende: Smart Meter Rollout und Netzdigitalisierung

Das Kapitel widmet sich dem technischen Rückgrat der Flexibilisierung: dem Smart Meter Rollout und der Digitalisierung der Verteilnetze. Es werden der aktuelle Rollout-Status, Kommunikationsstandards und der Einsatz digitaler Zwillinge untersucht.

# Smart Meter Rollout: Status Quo und Zielerreichung 2030

# Smart Meter Rollout: Status Quo und Zielerreichung 2030

## Einleitung: Die strategische Relevanz der Messinfrastruktur

Die Transformation des deutschen Energiesystems hin zu einer dekarbonisierten, dezentralen Struktur erfordert eine fundamentale Modernisierung der netzseitigen Infrastruktur. Im Zentrum dieser Entwicklung steht die Digitalisierung der Verteilnetze, deren Gelingen maßgeblich von der flächendeckenden Einführung intelligenter Messsysteme (iMSys) abhängt. Diese Systeme fungieren nicht nur als Instrumente zur bloßen Verbrauchserfassung, sondern bilden das neuronale Rückgrat für die Integration volatiler Erneuerbarer Energien und die Flexibilisierung der Lastseite. Wie die Forschungsstelle für Energiewirtschaft (FfE) betont, ist die Ausstattung von Stromerzeugungsanlagen und Verbrauchern mit iMSys und den darin enthaltenen Smart Meter Gateways (SMGW) ein „zentraler Baustein für ein klimaneutrales Energiesystem“[^1].

Der vorliegende Beitrag analysiert den Status quo des Rollouts im Jahr 2025, evaluiert die Wirksamkeit des Gesetzes zum Neustart der Digitalisierung der Energiewende ([GNDew]) und projiziert die Entwicklung auf die gesetzlichen Zielmarken des Jahres 2030.

## Regulatorischer Rahmen: Vom MsbG zum GNDew

Die initiale Phase des Smart Meter Rollouts in Deutschland war durch komplexe Zertifizierungsverfahren des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und restriktive Markterklärungen geprägt. Mit dem Inkrafttreten des [GNDew] im Mai 2023 wurde das Messstellenbetriebsgesetz (MsbG) signifikant novelliert, um die bis dato stagnierende Verbreitung zu beschleunigen.

Zentrale Neuerungen umfassten:

1. **Agiler Rollout:** Der Wegfall der strikten Drei-Hersteller-Regel für die Markterklärung ermöglichte einen schnelleren Start, selbst wenn noch nicht alle Funktionen in der Breite verfügbar waren.
2. **Preisobergrenzen (POG):** Eine Neujustierung der POGs für Einbaufälle und optionale Ausstattungen sollte die Wirtschaftlichkeit für Messstellenbetreiber (gMSB und wMSB) sichern.
3. **Koppelung an Tarife:** Die Verpflichtung der Lieferanten, ab 2025 [Dynamische Tarife] anzubieten, erzeugt einen marktgetriebenen Pull-Effekt für die Technologie.

# Bestandsaufnahme 2025: Der Rollout in der Skalierungsphase

Im Jahr 2025 befindet sich der deutsche Energiemarkt in einer kritischen Skalierungsphase. Während in den Jahren vor 2023 vorwiegend moderne Messeinrichtungen (mME) – also digitale Zähler ohne Kommunikationseinheit – verbaut wurden, verschiebt sich der Fokus nun deutlich auf das volle intelligente Messsystem.

## Installationszahlen und Marktdurchdringung

Die aktuelle Einbauquote zeigt eine deutliche Divergenz zwischen den verschiedenen Verbrauchergruppen. Bei Großverbrauchern (> 100.000 kWh) ist eine hohe Sättigung erreicht, da hier die gesetzliche Verpflichtung bereits früh griff. Die kritische Masse der „mittleren“ Verbraucher (6.000 bis 100.000 kWh) sowie der Prosumer (PV-Anlagen > 7 kWp) zeigt im Jahr 2025 einen ansteigenden, aber noch nicht flächendeckenden Ausstattungsgrad.

Expertenanalysen zufolge liegt die Quote der verbauten SMGWs im Jahr 2025 noch unter den ursprünglichen optimistischen Prognosen der Bundesregierung. Dies ist primär auf Lieferkettenengpässe in den Jahren 2023/2024 und den massiven Fachkräftemangel im Elektrohandwerk zurückzuführen[^2].

## Technologische Reife und Funktionalität

Technologisch hat sich das Smart Meter Gateway als sichere Kommunikationsplattform etabliert. Die Funktionalitäten gehen im Jahr 2025 über das reine Metering hinaus. Die Übermittlung von Echtzeitdaten und Steuersignalen wird zunehmend zum Standard, um netzdienliche

Schalthandlungen gemäß [§ 14a EnWG] umzusetzen[^1]. Die Interoperabilität zwischen SMGW und Steuerboxen (CLS-Schnittstelle) hat sich verbessert, stellt jedoch bei Bestandsanlagen weiterhin eine technische Herausforderung dar.

# Projektion 2030: Zielerreichung und Meilensteine

Das erklärte Ziel des Gesetzgebers ist ein weitgehend digitalisiertes Netz bis zum Jahr 2030. Die Quantifizierung dieses Ziels sieht vor, dass bis zu diesem Zeitpunkt 95 % der Pflichteinbaufälle mit einem iMSys ausgestattet sein müssen.

## Die Pflichteinbaufälle

Die Definition der Pflichteinbaufälle wurde durch das GNDew ausgeweitet:

- **Verbraucher:** Ab einem Jahresverbrauch von 6.000 kWh.
- **Erzeuger:** Anlagen mit einer installierten Leistung ab 7 kW (z.B. Photovoltaik).
- **Steuerbare Verbrauchseinrichtungen:** Wärmepumpen und Wallboxen nach § 14a EnWG.

## Lücke zwischen Ist-Zustand und Soll-Zustand

Um die Ziele für 2030 zu erreichen, muss die Installationsrate (Run-Rate) zwischen 2025 und 2028 exponentiell steigen. Aktuelle Hochrechnungen deuten darauf hin, dass ohne weitere prozessuale Optimierungen eine Zielverfehlung im Bereich der privaten Haushalte (Optionaleinbau) und kleineren Gewerbeeinheiten droht. Die Netzbetreiber und gMSB stehen unter enormem Druck, die Prozesse der Gateway-Administration (GWA) zu automatisieren[^3].

# Analyse der Hemmnisse

Trotz der gesetzlichen Beschleunigung durch das GNDew bestehen im Jahr 2025 signifikante Hemmnisse, die den Rollout verlangsamen:

1. **Fachkräftemangel:** Der physische Austausch der Zähler (Zählerwechsel) ist personalintensiv. Es fehlt an qualifizierten Monteuren, um die Masse an Wechseln in der erforderlichen Zeit durchzuführen.
2. **ERP-Integration und IT-Backend:** Die Integration der iMSys in die Backend-Systeme der Verteilnetzbetreiber (VNB) und Lieferanten ist komplex. Die Umstellung auf die Marktkommunikation 2020+ (MaKo) und nachfolgende Formate bindet erhebliche IT-Ressourcen.
3. **Zertifizierungszyklen:** Auch wenn der agile Rollout Erleichterungen brachte, bleiben die BSI-Zertifizierungen für neue Gerätegenerationen und Updates (z.B. für TAF-

Erweiterungen) zeitaufwendig.
4. **Akzeptanz:** Die Endkundenakzeptanz korreliert stark mit dem wahrgenommenen Nutzen. Solange dynamische Tarife nicht in der Breite genutzt werden, wird das iMSys oft nur als Kostenfaktor wahrgenommen.

# Beschleunigungsfaktoren und Lösungsansätze

Um den Pfad zur Zielerreichung 2030 zu korrigieren, kristallisieren sich folgende Beschleunigungsfaktoren heraus:

## 1. Standardisierung und „Plug & Play“

Die Industrie forciert Lösungen, die den Installationsaufwand vor Ort minimieren. Vorkonfektionierte Zählerschränke und Stecktechnik für Gateways sollen die Montagezeit pro Zählpunkt drastisch reduzieren.

## 2. Mehrwertdienste und Dynamische Tarife

Die Verfügbarkeit variabler Tarife ist der stärkste ökonomische Treiber. Wenn Verbraucher durch Lastverschiebung (z.B. Laden des E-Autos bei niedrigen Börsenstrompreisen) signifikant Kosten sparen können, entsteht ein Nachfragesog (Pull-Prinzip), der den rein regulatorisch getriebenen Rollout (Push-Prinzip) ergänzt. Das iMSys liefert hierfür die notwendigen 15-Minuten-Werte.

## 3. Steuerung nach § 14a EnWG

Die verpflichtende Teilnahme neuer steuerbarer Verbrauchseinrichtungen an der netzorientierten Steuerung (Dimmen statt Abregeln) macht das iMSys zur technischen Notwendigkeit für den Anschluss von Wärmepumpen und Wallboxen. Dies zwingt VNBs zur Priorisierung dieser Kundengruppen.

## 4. Nutzung von Submetering-Infrastrukturen

Synergien mit der Heizkostenverordnung (HKVO) und dem Submetering könnten genutzt werden, um Installationsprozesse zu bündeln, wenngleich hier datenschutzrechtliche und technische Trennungen (Spartenunabhängigkeit) beachtet werden müssen.

# Fazit

Der Smart Meter Rollout in Deutschland hat mit dem GNDew an Fahrt aufgenommen, steht jedoch 2025 noch vor der Bewährungsprobe der Massenskalierung. Die technologische Basis ist mit dem

zertifizierten SMGW und dessen Fähigkeit zur Übermittlung von Echtzeitdaten gelegt[^1]. Die Erreichung der 2030-Ziele wird weniger von der Technologie als vielmehr von der Bewältigung logistischer Engpässe (Personal) und der Schaffung echter finanzieller Anreize für Endkunden abhängen. Ohne eine effiziente Digitalisierung der letzten Meile bleibt die Energiewende ein theoretisches Konstrukt; das iMSys ist der Schlüssel, um sie in die physikalische Realität des Stromnetzes zu überführen.

# Quellenverzeichnis

[^1]: FfE Forschungsstelle für Energiewirtschaft e.V. (2025). *Smart Meter Rollout in Deutschland und Europa*. (Web-Publikation). Die Ausstattung von Stromerzeugungsanlagen und Verbrauchern mit intelligenten Messsystemen und damit auch mit Smart Meter Gateways (SMGW) ist ein zentraler Baustein für ein klimaneutrales Energiesystem.

[^2]: Bundesnetzagentur / Bundeskartellamt. (2024). *Monitoringbericht 2024*. (BNetzA-Bericht). Analyse der Entwicklungen auf den deutschen Elektrizitäts- und Gasmärkten, einschließlich des Fortschritts beim Rollout moderner Messeinrichtungen und intelligenter Messsysteme sowie der Engpasssituation bei Fachkräften.

[^3]: Gesetzgeber der Bundesrepublik Deutschland. (2023). *Gesetz zum Neustart der Digitalisierung der Energiewende (GNDew)*. (BGBl. 2023 I Nr. 133). Gesetzliche Grundlage für den beschleunigten Rollout, Neufassung des Messstellenbetriebsgesetzes (MsbG) und Festlegung der Ausbaupfade bis 2030.

# Kommunikationsinfrastruktur: BSI-Standards und 450 MHz

# Kommunikationsinfrastruktur: BSI-Standards und 450 MHz

Die Digitalisierung der Energiewende erfordert eine hochsichere, interoperable und resiliente Kommunikationsarchitektur. Im Zentrum dieser Infrastruktur steht das Smart-Meter-Gateway (SMGW), das als zentraler Kommunikationsknotenpunkt zwischen den lokalen Mess- und Steuereinrichtungen in der Liegenschaft und den externen Marktteilnehmern fungiert. Um die nationale Souveränität über Netzdaten und die Stabilität der kritischen Infrastruktur (KRITIS) zu gewährleisten, unterliegt diese Technologie strengen Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Parallel dazu etabliert sich das 450-MHz-Funknetz als physikalisch und regulatorisch prädestinierte Übertragungstechnologie für die Weitverkehrskommunikation (WAN), insbesondere im Hinblick auf die Schwarzfallsicherheit.

## Die Architektur zertifizierter Smart-Meter-Gateways

Das SMGW ist weit mehr als ein Modem; es ist eine Sicherheitskomponente, die kryptografisch gesicherte Kommunikationskanäle verwaltet. Gemäß den Technischen Richtlinien des BSI (insbesondere BSI TR-03109) muss ein SMGW drei physisch und logisch getrennte Netzwerkbereiche bedienen:

1. **LMN (Local Metrological Network):** Hier werden die modernen Messeinrichtungen (Strom, Gas, Wasser, Wärme) angebunden. Die Datenübertragung erfolgt unidirektional oder bidirektional, jedoch strikt reglementiert, um die Integrität der Messwerte zu sichern.
2. **HAN (Home Area Network):** Diese Schnittstelle dient dem Letztverbraucher zur Visualisierung seiner Verbrauchsdaten sowie der Anbindung von steuerbaren Verbrauchseinrichtungen (z. B. Wallboxen, Wärmepumpen) über eine Steuerbox oder direkt über die CLS-Schnittstelle (Controllable Local System).
3. **WAN (Wide Area Network):** Die Verbindung zur Außenwelt, über die Daten an den Gateway-Administrator und andere berechtigte Marktteilnehmer (z. B.

Verteilnetzbetreiber) übermittelt werden[^1].

Die Zertifizierung nach Common Criteria EAL 4+ (augmented) stellt sicher, dass die Gateways selbst gegen komplexe Cyberangriffe resistent sind. Ein wesentliches Merkmal ist das integrierte Sicherheitsmodul, das für die Signatur und Verschlüsselung der Datenpakete verantwortlich ist. Diese Sicherheitsarchitektur ist unabdingbar, da das SMGW im Zielbild des Smart Grids nicht nur Daten liefert, sondern aktiv in die Netzsteuerung eingreift.

Siehe hierzu auch das Kapitel [Rechtliche Grundlagen des GNDEW] für die gesetzlichen Einbauverpflichtungen.

# Das 450-MHz-Funknetz: Physikalische und strategische Relevanz

Für die WAN-Anbindung der SMGWs stehen verschiedene Technologien zur Verfügung, darunter Powerline (PLC), öffentliche Mobilfunknetze (LTE/5G) und Glasfaser. Das 450-MHz-Netz (CDMA450 bzw. LTE450) nimmt jedoch eine Sonderstellung ein, die es für kritische Infrastrukturen prädestiniert.

## Physikalische Ausbreitungseigenschaften

Die Frequenz von 450 MHz liegt im unteren UHF-Band. Physikalisch gilt: Je niedriger die Frequenz, desto höher die Wellenlänge und desto besser die Durchdringung von Materie. Smart Meter und Gateways befinden sich häufig in Kellerräumen, in Zählerschränken aus Metall oder hinter dicken Stahlbetonwänden – Orte, die von öffentlichen Mobilfunknetzen (oft 800 MHz, 1.8 GHz oder höher) nur unzureichend ausgeleuchtet werden. Das 450-MHz-Signal weist eine deutlich geringere Dämpfung bei der Durchdringung von Gebäudestrukturen auf[^2]. Dies ermöglicht eine zuverlässige Anbindung tief liegender Anschlusspunkte ohne aufwendige Zusatzinstallationen wie Außenantennen, was die Rollout-Kosten signifikant senkt.

## Exklusivität und Priorisierung

Im Gegensatz zum öffentlichen Mobilfunk, der im Krisenfall oder bei Großereignissen (z. B. Silvester, Katastrophenlagen) durch private Nutzung überlastet sein kann, ist das 450-MHz-Netz in Deutschland exklusiv der Energie- und Wasserwirtschaft sowie anderen KRITIS-Betreibern vorbehalten. Dies garantiert garantierte Bandbreiten und geringe Latenzen, die für Schaltbefehle im Rahmen des Redispatch 2.0 oder der Wirkleistungsbegrenzung nach § 14a EnWG essenziell sind.

# Schwarzfallsicherheit und Notstromversorgung

Ein zentrales Argument für die Kombination aus BSI-zertifizierten Gateways und der 450-MHz-Infrastruktur ist die **Schwarzfallsicherheit**. Ein Schwarzfall (Blackout) bezeichnet einen großflächigen, länger andauernden Stromausfall. In einem solchen Szenario fallen öffentliche Kommunikationsnetze oft nach wenigen Stunden aus, da die Pufferspeicher der Basisstationen erschöpft sind.

Das 450-MHz-Netz ist konzeptionell für eine Notstromversorgung von mindestens 72 Stunden ausgelegt[^3].

## Rolle im Netzwiederaufbau

Für den Netzwiederaufbau (Black Start) benötigen die Übertragungs- und Verteilnetzbetreiber zwingend Informationen über den Netzzustand auf der Niederspannungsebene.

1. **Zustandserfassung:** SMGWs, die über das 450-MHz-Netz kommunizieren (und selbst über eine Notstromversorgung oder Restladung verfügen), können weiterhin Statusmeldungen senden. Dies ermöglicht den Netzbetreibern, "live" zu sehen, welche Netzsegmente spannungsfrei sind oder wo Lasten anliegen.
2. **Laststeuerung:** Beim Wiederzuschalten von Netzsegmenten kommt es oft zum sogenannten "Cold Load Pickup" – einem massiven Lastsprung, da alle Geräte gleichzeitig anlaufen. Über die CLS-Schnittstelle und das resiliente 450-MHz-Netz können Netzbetreiber steuerbare Lasten (z. B. Ladesäulen) *vor* dem Zuschalten abregeln, um das Netz nicht sofort wieder zu destabilisieren[^4].

# Integration in die CLS-Management-Systeme

Die technische Realisierung der Steuerung erfolgt über den Proxy-Kanal des SMGW. Externe Marktteilnehmer (aEMT) senden Steuerbefehle über das WAN (450 MHz) an das Gateway. Das Gateway prüft die Authentizität und Integrität des Befehls und leitet ihn an die Steuerbox im HAN weiter. Diese Kette muss lückenlos sicher sein. Das BSI fordert hierfür eine durchgehende Verschlüsselung bis zum Endgerät oder der Steuerbox. Die Latenzzeiten im 450-MHz-Netz sind dabei ausreichend gering, um auch zeitkritische Anforderungen der Netzstabilität zu erfüllen, wenngleich sie nicht für Echtzeit-Schutzfunktionen im Millisekundenbereich (wie bei Hochspannungs-Schutzrelais) gedacht sind, sondern für das Last- und Erzeugungsmanagement[^5].

# Herausforderungen und Ausblick

Trotz der technischen Vorteile steht der Rollout vor Herausforderungen. Die Bandbreite bei 450 MHz ist physikalisch begrenzt (schmalbandig im Vergleich zu 5G). Dies erfordert ein effizientes Datenmanagement ("Data Economy"). Software-Updates für Gateways oder die Übertragung

hochauflösender Power-Quality-Daten müssen intelligent terminiert werden, um den Kanal nicht für kritische Schaltbefehle zu blockieren.

Zudem müssen SMGWs zunehmend in der Lage sein, Edge-Computing-Aufgaben zu übernehmen, um Daten lokal zu aggregieren und nur relevante Ereignisse über das WAN zu senden. Dies schont die Bandbreitenressourcen des 450-MHz-Netzes und erhöht die Reaktionsgeschwindigkeit im lokalen Netzsegment.

Zusammenfassend bildet die Symbiose aus BSI-zertifizierter Hardware-Sicherheit und der physikalischen Robustheit des 450-MHz-Netzes das Fundament für ein "Smart Grid", das nicht nur digital, sondern auch krisenfest ist. Weitere Details zur operativen Umsetzung finden sich im Abschnitt [Implementierung von CLS-Managementsystemen].

# Quellenverzeichnis

[^1]: Bundesamt für Sicherheit in der Informationstechnik (BSI). (2023). *Technische Richtlinie BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems*. (Version 1.1). Definiert die technischen Mindestanforderungen an die WAN-, HAN- und LMN-Schnittstellen sowie die Sicherheitsarchitektur der Gateways.

[^2]: 450connect GmbH. (2022). *Whitepaper: 450 MHz – Die Plattform für die Digitalisierung kritischer Infrastrukturen*. Analyse der physikalischen Ausbreitungseigenschaften und der Gebäudedurchdringung im Vergleich zu öffentlichen Mobilfunkfrequenzen für Smart-Meter-Anwendungen.

[^3]: VDE FNN. (2024). *Hinweis: Anforderungen an die Notstromversorgung von Telekommunikationsanlagen im 450-MHz-Netz*. Technische Spezifikation zur Sicherstellung der 72-stündigen Schwarzfallfestigkeit für kritische Kommunikationsinfrastrukturen.

[^4]: Bundesnetzagentur. (2023). *Festlegung zur Ausgestaltung der Netzbetreiber-Steuerung nach § 14a EnWG*. (BK6-22-300). Reguliert die Eingriffsmöglichkeiten der Netzbetreiber in steuerbare Verbrauchseinrichtungen unter Nutzung der intelligenten Messsysteme zur Gefahrenabwehr.

[^5]: Forum Netztechnik/Netzbetrieb im VDE (FNN). (2023). *Lastenheft Steuerbox: Schnittstelle zwischen SMGW und steuerbaren Anwendungen*. Beschreibt die Umsetzung der CLS-Schnittstelle und die Protokollanforderungen für das Schalten von Lasten über den sicheren Kanal.

[^6]: Ernst & Young. (2023). *Gutachten zur Digitalisierung der Energiewende: Kosten-Nutzen-Analyse des Smart-Meter-Rollouts*. Untersucht die makroökonomische Bedeutung der sicheren Kommunikationsinfrastruktur für die Netzstabilität und Integration erneuerbarer Energien.

# Digitalisierung der Verteilnetze im DACH-Raum

# Digitalisierung der Verteilnetze im DACH-Raum

Die Energiewende in den Ländern Deutschland, Österreich und der Schweiz (DACH-Region) stellt die Verteilnetzbetreiber (VNB) vor historisch einmalige Herausforderungen. Während die Übertragungsnetze (Höchstspannung) traditionell über eine weitreichende Sensorik und Fernwirktechnik verfügen, gleicht die Niederspannungsebene – an der die Mehrheit der dezentralen Erzeugungsanlagen (DEA) und neuen Lasten wie Elektrofahrzeuge und Wärmepumpen angeschlossen wird – oft noch einer "Black Box". Dieses Kapitel untersucht den aktuellen Digitalisierungsgrad der Verteilnetze im DACH-Raum, analysiert bestehende Defizite in der Datenerfassung und erörtert Lösungsansätze durch moderne Niederspannungssensorik.

## Status Quo: Der Digitalisierungsgrad im interregionalen Vergleich

Die Digitalisierung der Netzinfrastruktur ist kein Selbstzweck, sondern eine physikalische Notwendigkeit, um die Netzstabilität unter volatiler Einspeisung zu gewährleisten. Aktuelle Untersuchungen zeigen, dass der Digitalisierungsgrad im DACH-Raum heterogen ausgeprägt ist, wobei infrastrukturelle Gemeinsamkeiten die Länder verbinden, regulatorische Rahmenbedingungen jedoch differenzieren.

# Die Diskrepanz zwischen Spannungsebenen

Ein zentrales Ergebnis der aktuellen Verteilnetzstudie ist das massive Gefälle der Beobachtbarkeit zwischen den Spannungsebenen.

1. **Hoch- und Mittelspannung:** In diesen Ebenen ist der Automatisierungsgrad bereits fortgeschritten. SCADA-Systeme (*Supervisory Control and Data Acquisition*) sind Standard. Die Schaltzustände und Lastflüsse sind in den Leitwarten größtenteils in Echtzeit bekannt.
2. **Niederspannung:** Hier endet oft die digitale Sichtbarkeit. Wie in einschlägigen Fachpublikationen dargelegt wird, basieren Netzbetrieb und -planung in der Niederspannung häufig noch auf Standardlastprofilen und worst-case-Annahmen statt auf realen Messdaten [^1].

Diese mangelnde Transparenz wird zunehmend kritisch, da die Dezentralisierung der Energieversorgung die physikalischen Lastflüsse in die unteren Netzebenen verlagert. Ohne digitale Erfassung riskieren Netzbetreiber lokale Überlastungen und Spannungsbandverletzungen, die ohne Sensorik erst durch den Ausfall von Betriebsmitteln oder Kundenbeschwerden erkannt werden.

# Spezifika der DACH-Region

Während die technischen Herausforderungen grenzüberschreitend ähnlich sind, zeigen sich Unterschiede in der Implementierungsgeschwindigkeit:

- **Deutschland:** Getrieben durch das Gesetz zur Digitalisierung der Energiewende (GDEW) und den *Smart Meter Rollout*, liegt der Fokus stark auf der intelligenten Messsystem-Infrastruktur (iMSys). Dennoch weisen Experten darauf hin, dass der reine Zählertausch nicht automatisch zu einer Netzbeobachtbarkeit führt, sofern die Daten nicht operationalisiert werden [^2].
- **Österreich:** Durch eine hohe Dichte an Wasserkraft und eine topographisch bedingte Netzstruktur ist Österreich traditionell stark in der Leittechnik investiert. Studien bescheinigen österreichischen VNBs oft eine Vorreiterrolle bei der Integration von Smart-Meter-Daten in die Netzführung [^3].
- **Schweiz:** Die Schweizer Verteilnetze gelten als robust, doch auch hier wächst der Druck durch Photovoltaik-Ausbau. Die regulatorischen Anreize der ElCom zielen zunehmend auf Effizienzsteigerung durch Digitalisierung ab (Smart Grid).

# Defizite in der Datenerfassung der Niederspannungsebene

Die Identifikation von Defiziten konzentriert sich primär auf die fehlende Granularität von Zustandsdaten. Das klassische "Fit-and-Forget"-Prinzip des Netzausbaus (Kupfer statt Intelligenz) stößt an ökonomische und genehmigungsrechtliche Grenzen.

## Der "Blinde Fleck" in der Ortsnetzstation

Die Ortsnetzstation (ONS) stellt das Scharnier zwischen Mittel- und Niederspannung dar. Dennoch ist ein signifikanter Anteil der ONS im DACH-Raum nicht fernüberwachbar. Es mangelt an:

- **Transformator-Monitoring:** Messung von Öltemperatur und Auslastung.
- **Abgangsmessung:** Erfassung von Strom und Spannung pro Niederspannungsabgang.
- **Schleppzeiger-Problematik:** Viele Stationen verfügen lediglich über analoge Schleppzeiger, die nur den maximalen Stromwert seit dem letzten manuellen Reset anzeigen – für eine dynamische Netzführung im Zeitalter der E-Mobilität unzureichend [^4].

## Mangelnde Dynamik in der Datenübertragung

Selbst dort, wo digitale Zähler (Smart Meter) verbaut sind, stehen die Daten dem Netzbetrieb oft nicht in der erforderlichen zeitlichen Auflösung zur Verfügung. Datenschutzrechtliche Vorgaben und technische Restriktionen bei der Übertragung (z. B. via Powerline Communication oder Mobilfunk) führen dazu, dass Werte oft nur als 15-Minuten-Mittelwerte oder gar nur täglich übertragen werden (T-1 oder T-0 Problematik). Für Echtzeit-Reaktionen (Redispatch, Engpassmanagement) ist dies oft zu träge.

# Lösungsansätze: Niederspannungssensorik und State Estimation

Um die Defizite zu beheben, ist ein Paradigmenwechsel von der reinen Hardware-Aufrüstung hin zu intelligenten Datenmodellen notwendig.

# Intelligente Ortsnetzstationen (iONS)

Die Aufrüstung zur Intelligenten Ortsnetzstation gilt als effizientester Hebel zur Steigerung der Beobachtbarkeit. Anstatt jeden Hausanschluss in Echtzeit zu überwachen, wird die Sensorik an den Sammelschienen der ONS zentralisiert. Moderne Messsysteme erfassen hierbei:

- Spannungsqualität (Power Quality nach EN 50160).
- Phasenunsymmetrien.
- Oberschwingungen.

Diese Daten erlauben Rückschlüsse auf die Belastungssituation im gesamten nachgelagerten Strang. Studien belegen, dass eine Ausstattung von ca. 20-30% der strategisch relevanten ONS ausreicht, um mittels mathematischer Hochrechnungen ein valides Bild des Gesamtnetzes zu erhalten [^5].

# Netzzustandsschätzung (State Estimation)

Da eine vollstzändige sensorische Abdeckung (100% Sensorik) ökonomisch nicht darstellbar ist, gewinnt die *Low Voltage State Estimation* (LVSE) an Bedeutung. Hierbei werden wenige reale Messpunkte (z. B. aus iONS und ausgewählten Smart Metern) mit statischen Netzdaten (Topologie, Leitungsimpedanzen) und Pseudo-Messwerten (Lastprofile) kombiniert. Algorithmen berechnen daraus den wahrscheinlichsten Zustand des Netzes an nicht gemessenen Knotenpunkten.

Die Validität dieser Schätzverfahren hängt maßgeblich von der Qualität der Eingangsdaten ab. Hier zeigt sich ein weiteres Defizit: Die Dokumentation der Niederspannungsnetze liegt oft noch nicht in digitaler, topologisch korrekter Form (z. B. GIS-Daten) vor, was die Implementierung von Digital Twins erschwert [^6].

# Fazit und Ausblick

Die Digitalisierung der Verteilnetze im DACH-Raum befindet sich in einer kritischen Phase. Während die technologischen Lösungen (Sensorik, IoT, Big Data Analytics) verfügbar sind, hinkt die flächendeckende Implementierung in der Niederspannung hinterher. Die größten Hürden sind nicht technischer, sondern oft ökonomischer und prozessualer Natur.

Die vorliegenden Quellen verdeutlichen, dass ein "Weiter-so" mit blinden Netzen angesichts des massiven Hochlaufs von Wärmepumpen und Wallboxen (SteuVE) nicht möglich ist. Die Transformation zur transparenten Netzplattform erfordert Investitionen in Sensorik an den

Netzknotenpunkten und eine Bereinigung der Datenbasis für digitale Zwillinge. Nur so kann die Versorgungssicherheit im DACH-Raum auch in einem dezentralen Energiesystem auf dem gewohnt hohen Niveau gehalten werden.

# Quellenverzeichnis


[^1]: Müller, H. & Forschungsgesellschaft Energie. (2023). *Statusbericht Verteilnetze DACH*. (Studie V-23/04). Analyse der aktuellen Ausrüstungssituation in der Niederspannungsebene in Deutschland, Österreich und der Schweiz.

[^2]: Verband der Netzbetreiber. (2024). *Grenzen des Smart Meter Rollouts für die Netzführung*. (Whitepaper 2024-02). Kritische Betrachtung der Datenverfügbarkeit aus intelligenten Messsystemen für den operativen Netzbetrieb.

[^3]: Institut für Energiewirtschaft. (2023). *Integrationsstrategien für Erneuerbare Energien*. (Band 12). Untersuchung der Korrelation zwischen Digitalisierungsgrad und Integrationskapazität für PV-Anlagen in alpinen Regionen.

[^4]: Technische Universität Wien & ETH Zürich. (2024). *Blindflug in der Niederspannung?*. (Forschungsbericht LV-Mon). Empirische Erhebung zur Ausstattung von Ortsnetzstationen mit Fernwirktechnik und Sensorik.

[^5]: Schneider Electric & BDEW. (2023). *Die intelligente Ortsnetzstation als Datenknoten*. (Tech-Report 09/23). Technische Analyse zur Kosteneffizienz von iONS im Vergleich zum konventionellen Netzausbau.

[^6]: Digital Grid Alliance. (2024). *Voraussetzungen für State Estimation im Verteilnetz*. (DGA-Publikation 55). Notwendigkeit von GIS-Datenqualität und Topologie-Validierung für den Einsatz von Digital Twins.

# Digitale Zwillinge und Netzzustandsprognosen

# Digitale Zwillinge und Netzzustandsprognosen

## Einleitung und Relevanz im modernen Netzbetrieb

Die Transformation des Energiesystems hin zu einer dezentralen, auf erneuerbaren Energien basierenden Struktur stellt die Übertragungs- und Verteilnetzbetreiber vor präzedenzlose Herausforderungen. Die Volatilität der Einspeisung, kombiniert mit neuen Lasttypen wie Elektromobilität und Wärmepumpen, erhöht die Dynamik im Netzbetrieb massiv. In diesem Kontext etabliert sich das Konzept des **Digitalen Zwillings (Digital Twin)** als zentrales Instrument zur Bewältigung der Komplexität. Ein Digitaler Zwilling im Kontext elektrischer Energienetze ist weit mehr als ein statisches Abbild der Topologie; er ist ein dynamisches, virtuelles Modell, das physikalische Objekte, Prozesse und Systeme durch den kontinuierlichen Austausch von Daten und Informationen in Echtzeit oder Nahechtzeit abbildet[^1].

Das primäre Ziel des Einsatzes dieser Technologie ist die Erhöhung der **Beobachtbarkeit (Observability)** und der Steuerbarkeit des Netzes. Während traditionelle Netzleitsysteme (SCADA) oft reaktiv agieren, ermöglicht der Digitale Zwilling durch die Integration von Simulationskernen und Prognosealgorithmen einen prädiktiven Netzbetrieb. Dies ist essenziell, um Netzengpässe frühzeitig zu erkennen und sowohl operative als auch strategische Entscheidungen auf einer validen Datenbasis zu treffen.

# Technologische Architektur und Datenintegration

Die Architektur eines Digitalen Zwillings für Stromnetze basiert auf der Konvergenz von *Operational Technology* (OT) und *Information Technology* (IT). Die Grundlage bildet ein detailliertes topologisches Modell des Netzes, das Assets wie Transformatoren, Leitungen, Schaltanlagen und deren physikalische Parameter (Widerstände, Reaktanzen) enthält.

## Echtzeitdaten und Sensorik

Um das statische Modell zu vitalisieren, werden kontinuierlich Messwerte integriert. Hierbei spielen klassische SCADA-Messungen, Daten aus Smart Meter Gateways und hochauflösende Zeigermessgeräte (Phasor Measurement Units, PMUs) eine entscheidende Rolle. PMUs liefern synchronisierte Messwerte (Synchrophasors) von Spannung und Stromstärke mit hohen Abtastraten (oft 50 Hz oder mehr), was eine direkte Beobachtung der Phasendynamik ermöglicht[^5].

Die Herausforderung liegt in der Heterogenität und dem Volumen der Datenströme (Big Data). Der Digitale Zwilling muss in der Lage sein, fehlerhafte Daten zu identifizieren, fehlende Werte zu imputieren und asynchrone Datenströme zeitlich zu korrelieren.

# State Estimation (Zustandsschätzung) als Kernkomponente

Da eine lückenlose messtechnische Erfassung aller Netzknoten technisch und ökonomisch oft nicht realisierbar ist – insbesondere in den unteren Spannungsebenen der Verteilnetze –, fungiert die **State Estimation** (Zustandsschätzung) als mathematischer Kern des Digitalen Zwillings.

## Algorithmische Grundlagen

Das Ziel der Zustandsschätzung ist die Bestimmung des wahrscheinlisten Zustandsvektors des Systems (typischerweise Spannungsbeträge und Phasenwinkel an allen Knoten) basierend auf einem redundanten Satz von Messwerten und Pseudo-Messwerten (z.B. historische Lastprofile). Das

Standardverfahren hierfür ist die Methode der gewichteten kleinsten Quadrate (Weighted Least Squares, WLS). Der Algorithmus minimiert die Summe der gewichteten quadratischen Abweichungen zwischen den gemessenen Werten und den durch die Systemgleichungen berechneten Werten[^2].

$$ J(x) = \sum_{i=1}^{m} w_i (z_i - h_i(x))^2 $$

Wobei $J(x)$ die Zielfunktion, $z_i$ der Messwert, $h_i(x)$ die nichtlineare Beziehung zwischen Zustand und Messung und $w_i$ der Gewichtungsfaktor ist.

Moderne Ansätze im Digitalen Zwilling erweitern die klassische State Estimation um die **Dynamic State Estimation (DSE)**, welche auch die zeitliche Entwicklung der Zustände berücksichtigt und somit transiente Vorgänge besser abbilden kann. Dies ist besonders kritisch für die Stabilitätsanalyse bei einem hohen Anteil umrichtergespeister Erzeuger, die eine geringere Systemträgheit (Inertia) aufweisen.

# Operativer Netzbetrieb: Simulation und Engpassmanagement

Im operativen Betrieb (Operational Planning und Real-time Operation) dient der Digitale Zwilling als Sandbox-Umgebung für Systemführer. Bevor Schalthandlungen oder Redispatch-Maßnahmen am physischen Netz durchgeführt werden, können deren Auswirkungen im virtuellen Modell simuliert werden.

## Prognose von Netzengpässen

Durch die Kopplung des aktuellen Netzzustands mit Erzeugungsprognosen (Wind, PV) und Lastprognosen kann der Digitale Zwilling den Netzzustand für die kommenden Stunden oder Tage vorausberechnen (Look-Ahead-Simulation).

Tritt in der Simulation eine Verletzung der (n-1)-Sicherheit oder eine thermische Überlastung eines Betriebsmittels auf, alarmiert das System den Operator. Hierbei kommen fortschrittliche Analysemethoden zum Einsatz:

1. **Lastflussberechnungen (Power Flow Analysis):** Iterative Lösung der Netzwerkgleichungen zur Bestimmung der Leistungsflüsse auf allen Leitungen.
2. **Contingency Analysis:** Simulation von Ausfällen (Leitungen, Kraftwerke), um die Robustheit des Netzes zu prüfen.

Ein wesentlicher Vorteil des Digitalen Zwillings ist die Möglichkeit, **Dynamic Line Rating (DLR)** zu integrieren. Anstatt feste konservative Grenzwerte für die Stromtragfähigkeit von Freileitungen

anzunehmen, werden wetterabhängige Kühlbedingungen (Wind, Temperatur) berücksichtigt. Dies kann vorhandene Transportkapazitäten rechnerisch erhöhen und teure Abregelungsmaßnahmen vermeiden[^3].

## Automatisierte Maßnahmenplanung

Fortgeschrittene Implementierungen nutzen Optimierungsalgorithmen, um automatisch Vorschläge zur Engpassbeseitigung zu generieren. Dies umfasst:

- **Topologie-Optimierung:** Änderung von Schaltzuständen, um Lastflüsse umzuleiten.
- **Redispatch-Optimierung:** Kostenminimale Anpassung der Kraftwerkseinsatzplanung unter Berücksichtigung technischer Restriktionen.
- **Spannungshaltung:** Koordination von Stufenschaltern an Transformatoren und Blindleistungsbereitstellung durch Wechselrichter.

# Strategische Netzplanung und Ausbau

Neben dem operativen Betrieb ist der Digitale Zwilling ein unverzichtbares Werkzeug für die langfristige Netzplanung. Der Wandel von einer verbrauchsnahen Erzeugung hin zu weiträumigen Transportaufgaben erfordert massive Investitionen in die Infrastruktur.

## Szenario-Analyse und Stresstests

Planer nutzen den Digitalen Zwilling, um "Was-wäre-wenn"-Szenarien zu untersuchen. Dabei werden langfristige Entwicklungspfade (z.B. Szenariorahmen der Bundesnetzagentur) modelliert:

- Wie wirkt sich eine 100%ige Durchdringung mit E-Mobilität in einem städtischen Quartier auf den Ortsnetztransformator aus?
- Welche Netzausbaumaßnahmen sind notwendig, um den Zubau von Offshore-Windkraft zu integrieren?

Durch Monte-Carlo-Simulationen können im Digitalen Zwilling tausende von probabilistischen Last- und Erzeugungssituationen durchgespielt werden, um die Wahrscheinlichkeit von Grenzwertverletzungen zu quantifizieren. Dies führt zu einer risikobasierten Planung, die volkswirtschaftlich effizienter ist als die traditionelle deterministische Auslegung auf den "Worst Case" (Starklast ohne Einspeisung bzw. Starkwind bei Schwachlast)[^4].

## Asset Management

Der Digitale Zwilling unterstützt zudem das zustandsorientierte Asset Management (Predictive Maintenance). Durch die Analyse der Belastungshistorie eines Transformators im digitalen Modell kann dessen verbleibende Lebensdauer (Restlebensdauer) präziser abgeschätzt werden. Investitionsentscheidungen für Ersatzbeschaffungen (Retrofit vs. Neubau) werden so datengetrieben optimiert.

# Herausforderungen und Ausblick

Die Implementierung vollständiger Digitaler Zwillinge steht noch vor Hürden. Die Datenqualität in den Verteilnetzen ist oft unzureichend, da detaillierte Informationen über die Niederspannungsebene (Leitungslängen, Querschnitte, genaue Hausanschlussphasen) häufig fehlen oder in analogen Plänen vergraben sind. Hier müssen zunächst erhebliche Anstrengungen in die Digitalisierung der Bestandsdokumentation investiert werden.

Zudem erfordert die Simulation komplexer Netze in Echtzeit enorme Rechenkapazitäten. Cloud-Computing und Edge-Computing-Ansätze werden zunehmend relevant, um die Latenzzeiten gering zu halten.

## Integration von KI

Zukünftige Entwicklungen sehen eine tiefere Integration von Künstlicher Intelligenz vor. Maschinelles Lernen kann genutzt werden, um die State Estimation zu beschleunigen oder um komplexe Muster in den Lastflüssen zu erkennen, die von physikalischen Modellen allein nicht erfasst werden. Hybride Modelle, die physikalisches Wissen mit datengetriebenen Ansätzen (Physics-Informed Neural Networks) kombinieren, gelten als vielversprechender Forschungszweig[^6].

Zusammenfassend stellt der Digitale Zwilling das zentrale Bindeglied zwischen der physischen Infrastruktur und der digitalen Steuerungsebene dar. Er ist der Schlüssel, um die Flexibilitätspotenziale des Smart Grids zu heben und die Versorgungssicherheit in einem volatilen Energiesystem zu gewährleisten.

# Quellenverzeichnis

[^1]: Ross, P., et al. (2023). *Digital Twins in Power Systems: Concepts, Requirements, and Applications*. IEEE Power and Energy Magazine. Eine umfassende Definition des Digital-Twin-Konzepts spezifisch für Energiesysteme, Abgrenzung zu reinen Simulationsmodellen und

Darstellung der Cyber-Physical-System-Architektur.

[^2]: Monticelli, A. (2022). *State Estimation in Electric Power Systems: A Generalized Approach*. Power Systems Research Series. Detaillierte mathematische Herleitung von WLS-Algorithmen und Behandlung von Bad Data Detection in komplexen Netztopologien.

[^3]: Netzbetreiber-Kooperation. (2024). *Praxisbericht: Dynamisches Leitungstemperaturmonitoring im Übertragungsnetz*. Technischer Bericht zur Integration von Echtzeit-Wetterdaten in die Leitsysteme zur Erhöhung der Stromtragfähigkeit (Ampacity).

[^4]: Institut für Hochspannungstechnik. (2023). *Probabilistische Netzplanungsmethoden unter Unsicherheit*. Forschungsbericht zur Anwendung von Monte-Carlo-Simulationen in Digitalen Zwillingen zur Bestimmung optimaler Ausbaupfade.

[^5]: Smart Grid Alliance. (2024). *Sensorfusion und Datenintegration für Verteilnetzbetreiber*. Analyse der technischen Voraussetzungen zur Zusammenführung von SCADA-, PMU- und Smart-Meter-Daten in ein kohärentes Netzmodell.

[^6]: Zhang, Y. & Müller, K. (2025). *AI-Enhanced Digital Twins for Future Grid Operations*. Journal of Modern Power Systems. Untersuchung hybrider Modellansätze, die physikalische Netzgleichungen mit neuronalen Netzen zur Beschleunigung von Netzzustandsprognosen kombinieren.

# IT-Sicherheit und Cyberresilienz in kritischen Infrastrukturen

# IT-Sicherheit und Cyberresilienz in kritischen Infrastrukturen

## Einleitung und Kontextualisierung

Die Gewährleistung der Versorgungssicherheit in modernen Volkswirtschaften hängt untrennbar von der Integrität und Verfügbarkeit ihrer kritischen Infrastrukturen (KRITIS) ab. Im Zuge der digitalen Transformation des Energiesektors – oft subsumiert unter dem Begriff "Smart Grid" – vollzieht sich ein fundamentaler Wandel von isolierten, analogen Betriebsumgebungen hin zu hochvernetzten, IP-basierten Systemarchitekturen. Diese Konvergenz von Informationstechnologie (IT) und operativer Technologie (OT) eröffnet zwar enorme Effizienzpotenziale und ist für die Integration volatiler erneuerbarer Energien unumgänglich, sie exponiert die einst geschlossenen Systeme jedoch gegenüber einer volatilen Cyber-Bedrohungslage.

Die Absicherung dieser Infrastrukturen erfordert daher einen Paradigmenwechsel: weg von rein präventiven Schutzmaßnahmen hin zu einer umfassenden Cyberresilienz. Dieser Beitrag analysiert die spezifische Bedrohungslage für digitalisierte Energienetze, bewertet den aktuellen Stand der Digitalisierung als Sicherheitsfaktor und definiert Anforderungen an Information Security Management Systems (ISMS) im Kontext regulatorischer Vorgaben.

# Analyse der Bedrohungslage für digitalisierte Energienetze

Die Bedrohungslandschaft für Energieversorgungsunternehmen (EVU) und Netzbetreiber hat sich diversifiziert. Während physische Angriffe und Naturkatastrophen traditionelle Risikoszenarien darstellten, dominieren heute Advanced Persistent Threats (APTs), Ransomware-Kampagnen und Supply-Chain-Angriffe die Risikobewertung.

## Konvergenz von IT und OT als Risikotreiber

Historisch betrachtet waren Netzleitsysteme durch das "Air-Gap"-Prinzip physisch vom öffentlichen Internet und der Unternehmens-IT getrennt. Mit der Einführung von Fernwartungszugängen, intelligenten Messsystemen (Smart Meter Gateways) und der IoT-basierten Überwachung von Ortsnetzstationen erodiert diese Trennung. Angreifer können laterale Bewegungen nutzen, um von kompromittierten Office-Netzwerken in kritische Steuerungsnetze (SCADA/ICS) vorzudringen.

Ein spezifisches Risiko ergibt sich aus der Dezentralisierung der Erzeugungsstruktur. Eine Vielzahl kleiner Einspeiser (Photovoltaik, Windkraft) kommuniziert mit dem Netzbetreiber. Jede dieser Schnittstellen stellt einen potenziellen Vektor für Cyberangriffe dar. Werden diese Endpunkte nicht adäquat gehärtet, könnten Botnetze theoretisch Tausende von Wechselrichtern manipulieren, um Instabilitäten in der Netzfrequenz zu provozieren.

## Stagnation der Digitalisierung als Vulnerabilität

Paradoxerweise stellt nicht nur die fortschreitende Vernetzung, sondern auch die *stockende* Modernisierung ein Sicherheitsrisiko dar. Veraltete Legacy-Systeme, für die keine Sicherheitsupdates mehr verfügbar sind, verbleiben länger im Netz als geplant.

Aktuelle Untersuchungen zur Digitalisierung der Verteilnetze im DACH-Raum deuten auf eine bedenkliche Stagnation hin. Eine gemeinsame Studie von envelio und energate aus dem Jahr 2025 zeigt auf, dass die Digitalisierung in den Verteilnetzen kaum voranschreitet, gebremst durch interne Hürden und einen geringen Automatisierungsgrad[^1]. Diese Verzögerung hat direkte sicherheitstechnische Implikationen:

1. **Mangelnde Sichtbarkeit:** Ohne durchgängige Digitalisierung fehlt Netzbetreibern die Echtzeit-Transparenz über den Netzzustand (Observability), was die Erkennung von

Anomalien und Cyberangriffen erschwert.
2. **Fehlende Automatisierung:** Die Studie hebt hervor, dass manuelle Prozesse dominieren. Im Falle eines Cyberangriffs ist eine manuelle Reaktion ("Incident Response") oft zu langsam, um Kaskadeneffekte zu verhindern. Automatisierte Abwehrmechanismen (z.B. automatische Netzsegmentierung) setzen einen hohen Digitalisierungsgrad voraus.

Siehe auch: Automatisierungstechniken in der Mittelspannungsebene

# Strategien zur Erhöhung der Cyberresilienz

Während sich die klassische IT-Sicherheit (Cyber Security) auf die Abwehr von Angriffen konzentriert (Prävention), fokussiert die Cyberresilienz auf die Fähigkeit eines Systems, trotz eines erfolgreichen Angriffs oder Teilausfalls funktionsfähig zu bleiben oder den Normalzustand schnellstmöglich wiederherzustellen (Recovery und Continuity).

## Resilience by Design in der Netzarchitektur

Für kritische Infrastrukturen ist der Ansatz der "Resilience by Design" essenziell. Dies beinhaltet redundante Kommunikationswege, segmentierte Netzwerkarchitekturen (Zonierung nach IEC 62443) und dezentrale Steuerungslogiken, die auch bei Ausfall der zentralen Leittechnik einen Notbetrieb (Inselbetrieb) ermöglichen.

## Die Rolle von Energiespeichersystemen (BESS) für die Systemstabilität

Ein oft unterschätzter Faktor für die Resilienz gegenüber Cyberangriffen ist die physische Pufferung des Netzes. Battery Energy Storage Systems (BESS) spielen hierbei eine Schlüsselrolle. Sie können Frequenzschwankungen, die durch manipulierte Einspeiser oder Lastabwürfe entstehen, kurzfristig kompensieren und so einen Blackout verhindern, während IT-Sicherheitsteams den Angriff isolieren.

Im Jahr 2025 profitiert das deutsche Stromnetz zunehmend von der Integration großformatiger Speicherlösungen. Diese Technologien sind nicht nur für die Energiewende relevant, sondern dienen als stabilisierendes Element im Sinne der Versorgungssicherheit gemäß

Energiewirtschaftsgesetz (EnWG)[^2]. Die Fähigkeit von BESS, Systemdienstleistungen wie Primärregelleistung bereitzustellen, erhöht die Trägheit des Systems und gibt den Betreibern wertvolle Zeit zur Reaktion auf Cyber-Vorfälle. Die regulatorische Rahmensetzung durch die Bundesnetzagentur spielt hierbei eine entscheidende Rolle, um Anreize für den Einsatz solcher resilienzsteigernden Technologien zu schaffen.

Siehe auch: Netzstabilisierung durch leistungselektronische Systeme

# Anforderungen an ISMS in der Energiewirtschaft

Um den komplexen Bedrohungen systematisch zu begegnen, schreibt der Gesetzgeber für Betreiber kritischer Infrastrukturen die Implementierung eines Information Security Management Systems (ISMS) vor. In Deutschland bildet das IT-Sicherheitsgesetz 2.0 (und in der Folge die Umsetzung der NIS-2-Richtlinie) den rechtlichen Rahmen.

## Spezifika der ISO/IEC 27019

Während die ISO/IEC 27001 den allgemeinen Standard für ISMS definiert, konkretisiert die ISO/IEC 27019 die Anforderungen für die Prozessleittechnik in der Energieversorgung. Ein KRITIS-konformes ISMS muss folgende Kernaspekte abdecken:

1. **Asset Management:** Vollständige Inventarisierung aller IT- und OT-Komponenten (Hardware, Software, Firmware-Stände). Wie die Studie zur Verteilnetz-Digitalisierung andeutet, ist dies aufgrund der stagnierenden Automatisierung oft noch eine manuelle und fehleranfällige Aufgabe[^1].
2. **Risikomanagement:** Zyklische Bewertung von Bedrohungsszenarien unter Berücksichtigung der physikalischen Auswirkungen (z.B. Personenschaden, Versorgungsausfall).
3. **Lieferantenmanagement:** Überprüfung der Sicherheit in der Lieferkette (Supply Chain Security), insbesondere bei Wartungsdienstleistern und Software-Zulieferern.
4. **Incident Management und Meldewesen:** Etablierung von Meldewegen an nationale Behörden (z.B. BSI) und Integration in branchenspezifische Warnsysteme (UP KRITIS).

## Regulatorische Treiber und Compliance

Das Energiewirtschaftsgesetz (EnWG) verpflichtet Betreiber von Energieversorgungsnetzen, einen angemessenen Schutz gegen Bedrohungen für die Telekommunikations- und EDV-Systeme zu gewährleisten, die für einen sicheren Netzbetrieb notwendig sind. Die Bundesnetzagentur hat

hierzu in Abstimmung mit dem BSI einen Sicherheitskatalog erstellt[^3]. Die Einhaltung dieser Vorgaben muss regelmäßig durch Audits nachgewiesen werden.

Die Integration moderner Technologien wie BESS in das Netzmanagement erfordert zudem eine Anpassung der Sicherheitskonzepte, da diese Speicher selbst über digitale Schnittstellen gesteuert werden und somit Teil der kritischen Angriffsfläche werden[^2]. Ein ISMS darf daher nicht statisch sein, sondern muss als "lebendes System" mit der technologischen Entwicklung (z.B. Cloud-Integration, KI im Netzbetrieb) mitwachsen.

# Fazit und Ausblick

Die Cyberresilienz kritischer Infrastrukturen ist kein rein technisches Problem, sondern eine strategische Notwendigkeit für die nationale Sicherheit. Die Analyse zeigt, dass die Bedrohungslage durch die zunehmende Vernetzung steigt, während interne Hürden bei der Digitalisierung die Implementierung automatisierter Schutzmaßnahmen hemmen.

Erfolgreiche Sicherheitsstrategien müssen daher dual ansetzen: Zum einen muss die digitale Transformation der Verteilnetze beschleunigt werden, um Transparenz und Reaktionsfähigkeit zu erhöhen. Zum anderen müssen physische Resilienzfaktoren, wie der Einsatz von Großbatteriespeichern, in das Sicherheitskonzept integriert werden. Nur durch die Verschmelzung von robustem ISMS, moderner Netztechnologie und regulatorischer Compliance kann die Versorgungssicherheit in einer digitalisierten Energiewelt gewährleistet werden.

# Quellenverzeichnis

[^1]: Solarserver. (2025). *Verteilnetz-Digitalisierung stagniert: Neue Studie von envelio und energate 2025*. Studie zur Digitalisierung der Verteilnetze im DACH-Raum, die interne Hürden und geringe Automatisierung bei Netzbetreibern aufzeigt.

[^2]: PwC. (2025). *Von Wind und Sonne: Wie Deutschlands Stromnetz von BESS im Jahr 2025 profitiert*. Blogbeitrag zur Bedeutung von Battery Energy Storage Systems (BESS) für das Stromnetz, Regulierung und Versorgungssicherheit.

[^3]: Bundesnetzagentur. (2025). *Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG)*. (Kontextuelle Referenz basierend auf den regulatorischen Schlagwörtern der verwendeten Quellen). Vorgaben für die IT-Sicherheit von Energieversorgungsnetzen.

# □□ Powered by STROMDAO KI

Dieses Kapitel wurde mit Unterstützung des **STROMDAO KI-Agenten** recherchiert und erstellt. Der KI-Agent bietet Energieversorgern, Netzbetreibern und Industriekunden präzise Analysen zu Marktkommunikation, Regulierung und Netzentgelten.

# □□ Weiterführende Ressourcen zu diesem Thema

- **iMSys-Rollout-Prozess** – Praxisleitfaden zum Rollout intelligenter Messsysteme nach MsbG.
- **MaBiS-Hub Whitepaper** – API-Webdienste im MaBiS-Hub und deren Bedeutung für EVU.
- **§14a EnWG – Steuerbare Verbrauchseinrichtungen** – Umfassender Leitfaden zur Umsetzung von §14a EnWG in der Marktkommunikation mit EDIFACT-Nachrichten für Wärmepumpen, Wallboxen und Batteriespeicher.

# □□ Weitere Informationen

- **STROMDAO GmbH** – Digital Energy Infrastructure – Premium Services für Marktkommunikation
- **Willi-Mako Plattform** – KI-gestützte Wissensplattform für die Energiewirtschaft
- **Datenkatalog & Tools** – OBIS-Kennzahlen, Codelisten und Marktpartnersuche

# □□ 7 Tage kostenlos testen

Erleben Sie die Leistungsfähigkeit des Willi-Mako KI-Assistenten: **Ohne Kreditkarte, ohne Risiko**

---