



BSKI THINK TANK

Leitung: Miriam Schnürer, Dr. Hans-Walter Borries

Arbeitspapier:

„Stromausfall“:

**Die resiliente Zelle/das resistente Quartier –
Strategische Impulse für eine zellulare
Infrastrukturwende**

Stand: 13.01.2026

BSKI-Think Tank Arbeitspapier:**„Stromausfall“: Die resiliente Zelle/das resistente Quartier –
Strategische Impulse für eine zelluläre Infrastrukturwende**

Autoren: BSKI Think Tank unter der Leitung: Miriam Schnürer, Dr. Hans-Walter Borries

I. Die Lage: Physische Vulnerabilität im 21. Jahrhundert

Der Brandanschlag auf das Berliner Stromnetz war kein lokaler Störfall, sondern ein systemisches Warnsignal. Rund 45.000 Haushalte und 2.200 Betriebe waren über mehrere Tage betroffen – nach Anzahl der Betroffenen und Dauer einer der längsten dokumentierten städtischen Ausfälle in Berlin.

Der stellvertretende Vorsitzende des BSKI Dr. Borries warnt: „Wer sich mit Stromleitungen auskennt, findet überall in Deutschland unzureichend geschützte Anschlagssziele.“ Das Netz ist historisch für Normalbetrieb und technische Störungen optimiert – nicht für gezielte Sabotage und hybride Angriffslagen. Klassische Redundanz kann als Common-Mode-Failure versagen, wenn Leitungsstränge parallel geführt oder an wenigen Knoten konzentriert sind.

Da eine flächendeckende physische Härtung in der Breite ökonomisch unrealistisch ist, muss der Schutz der Funktion über den Schutz der Leitung gestellt werden. Zudem wird Resilienz zunehmend ein Versicherungs- und Finanzierungsfaktor: Fehlende oder nicht getestete Notbetriebskonzepte erhöhen das Risiko steigender Prämien und können Ausschlüsse begünstigen – ein Trend, der sich in der Versicherungswirtschaft abzeichnet.

II. Coupled System Governance: Layer und Tier (siehe Lit. Hinweise)

Wir trennen explizit zwischen Struktur (Layer) und Autorität (Tier):

6-Layer-Modell (WAS): Geo, Infrastructure, Control & Logic, Data, Process, Governance.

Multi-Tier-Logik (WO): Zentral (Backbone) → Regional (Hub) → Edge (Lokal).

Spezifikation der Edge-Intelligenz

Control & Logic: Einsatz eines deterministischen Safety-Controllers (Safety-PLC oder Microgrid-Controller nach IEC 61508/IEC 61850). Er sichert den physikalischen Übergang ab und verhindert Instabilitäten beim Hochfahren – insbesondere Lastspitzen durch unkontrolliertes gleichzeitiges Einschalten.

Data Layer: Kritische Parameter, Lastklassen-Profile und Betriebszustände müssen am Edge-Knoten lokal vorliegen (pre-loaded Snapshots), um bei Netztrennung sofort autonom handlungsfähig zu sein.

Trust Plane: Dezentrale Autorität erfordert digitale Souveränität gegen Cyber-Sabotage (orientiert an IEC 62443 für Industrial Security). Nur kryptographisch signierte Befehle werden ausgeführt. Hardware-basierte Attestierung (z. B. TPM) verifiziert mobile Einspeisungen und Steuerungskomponenten. Ein hierarchisches PKI-Modell mit offline-fähigen lokalen Autoritäten ermöglicht es dem Edge, auch ohne zentrale Infrastruktur Entscheidungen zu validieren. Alle Schalthandlungen werden manipulationssicher protokolliert (z. B. via WORM-Speicher oder HSM-signierte Logs).

III. Berlin als Demonstrator: Die Kopplungskette

Der Berlin-Fall zeigt, wie ein urbanes System unter Stress reagiert:

Infrastructure: Konzentration kritischer Knoten; begrenzte physische Segmentierung.

Control & Logic: Das Fehlen automatisierter Lastpriorisierung wird sichtbar, wenn Behörden nach Wiederschaltung explizit darum bitten müssen, keine Großverbraucher sofort hochzufahren – ein Indiz für fehlende technische Abfanglogik des „Wiedereinschalt-Schocks“.

Data/Process/Governance: Fragmentiertes Lagebild, Ad-hoc-Maßnahmen, Zuständigkeits- und Schwellenlogiken erzeugen Resilienz-Lücken.

Schlussfolgerung: Resilienz ist keine Einzelschutzmaßnahme, sondern die Fähigkeit, gekoppelte Schichten unter Stress kontrolliert zu betreiben.

IV. Politische Forderung: Resilienz als Planungsstandard

Wir regen beispielhaft folgende Hebel zur Absicherung urbaner Zentren an:

Ringfähige Planung: Segmentierbare, fernschaltbare Netzstrukturen für Neubauquartiere zur gezielten Abschnittsbildung (nicht „Vermaschung“ als Schlagwort, sondern operationalisierbare Segmentierung). Dies erfordert abgestimmte Vorgaben zwischen Netzbetreibern, Kommunen und Bauträgern.

Versorgungs-Nexus (Strom/Wasser/Wärme): Gemeinsame Planung inkl. thermischer Speicher und Notwärmepfaden, um die „elektrische Wärmefalle“ im Winter zu umgehen.

Docking-Port-Standard: Standardisierte, normkonforme Notstromeinspeisepunkte (orientiert an VDE-AR-N 4100 für Erzeugungsanlagen; spezifische Normen für mobile Einspeisung befinden sich in Entwicklung), um mobile Ressourcen (THW-Aggregate, Container-Batterien, E-Flotten) sofort anschlussfähig zu machen.

Bemessungsfall 72h-Autarkie: Nachweisbare Stabilität der Vitalfunktionen über drei Tage – anschlussfähig an EU-Preparedness-Leitlinien („minimum 72 hours“) und nationale Vorsorgeempfehlungen.

V. Energie auf die Straße: Das E-Bus-Konzept (Beispielhafter Lösungsansatz)

Leitungsgebundene Versorgung kann zum Single Point of Failure werden. Ergänzend zur Netzsegmentierung entsteht Resilienz durch logistische Flexibilität. Moderne E-Busse fungieren als mobile Energietransporteur: Mercedes-Benz eCitaro G bis 777 kWh, Solaris Urbino 18 electric über 800 kWh (konfigurationsabhängig).

Einsatzlogik

- Fahrt zum Resilienz-Ladehub außerhalb der Störzone (Depot-/Hub-Infrastruktur mit gesicherter Einspeisung und/oder eigener Notversorgung)
- Rückführung und Einspeisung an kritischen Zellen (Pflegeheime, Krankenhäuser, Wärmeräume)
- Bis zu 24h Vitalversorgung für ca. 100–150 Personen pro Bus (bei 15–20 kW Notbetrieb ohne Heizlast, abhängig von Ladezustand und Umgebungsbedingungen)

Technischer Pfad

Mobile Energie wird nicht „direkt“ eingespeist, sondern über:

- Geeignete Leistungselektronik (PCS/Wechselrichter) für Inselbetrieb (idealerweise netzbildend)
- Normkonforme Umschalt- und Schutzlogik am Docking-Port
- Deterministische Steuerlogik (wer dockt wo wann an; Priorisierung nach Lastklassen)

Die Umsetzung erfordert koordinierte Freigaben zwischen Fahrzeugherstellern, Ladeinfrastruktur und Netzbetreibern. Bidirektionales Laden und Vehicle-to-Grid-Kommunikation werden durch Normen wie ISO 15118-20 adressiert.

Randbedingungen

Die praktische Umsetzung setzt voraus: resiliente, blackstart-fähige Ladehubs, verfügbares Fachpersonal, und klare Priorisierung zwischen Transport- und Energieeinsatz im Krisenfall. Ladezeit und kW-Abgabeleistung müssen in der Einsatzplanung berücksichtigt werden.

Ökonomische Effizienz

Die Infrastruktur kann sich durch Doppelnutzung im Normalbetrieb amortisieren (ÖPNV + netzdienliche Leistungen wie Peak-Shaving). Resilienz wird zum aktiven Asset, nicht zum toten Kapital. Die genaue Wirtschaftlichkeit hängt von regulatorischen Rahmenbedingungen und Netzentgeltregimen ab.

„Wir müssen den Strom auf die Straße bringen. Jede E-Bus-Flotte ist ein rollendes Kraftwerk, das wir dorthin dirigieren können, wo das Leben geschützt werden muss.“ — **Marten Jensen, GreenTEC Campus, auf dem Campus sind proof of concept Modelle (Autarke Bevölkerungs Infrastruktur System) erprobt worden und können besichtigt werden.**

VI. Wärme-Realismus und thermische Trägheit

Wärme ist der dominante Lasttreiber im Winter. Wenn ein Inselnetz hochfährt und viele Wärmepumpen unkontrolliert anlaufen, kollabiert das System. **Thermische Trägheit ist Resilienz-Infrastruktur:**

- **Gebäudephysik:** Hoher Dämmstandard, massive Bauweise – Wärme halten, nicht nur erzeugen
- **Thermische Speicher:** Pufferspeicher, Bauteilaktivierung, ggf. saisonale Speicher
- **Lastmanagement:** Gestaffelte Anlauflogik, Priorisierung von Life-Safety-Bereichen

Notwärmepfad: Brennstoffgesicherte Optionen

Je nach Quartierstyp und verfügbarer Infrastruktur:

- **Diesel-basiert:** HVO-fähige Notstromaggregate zur Stromerzeugung (für Pumpen, Steuerung, Hilfsenergie; nicht für elektrische Direktheizung, da dies die Lastfalle verschärft)
- **Gas-basiert:** BHKW mit gesicherter Gasversorgung (Kraft-Wärme-Kopplung, ideal für gleichzeitige Wärme- und Stromerzeugung)
- **Hybrid:** Dual-Fuel-Aggregate (können zwischen Gas und Diesel wechseln, maximale Flexibilität bei unsicherer Brennstoffverfügbarkeit)

Entscheidend: Der Brennstoffpfad muss vor Ort verfügbar, betriebssicher und im Krisenfall zugänglich sein.

Notbetrieb muss Lebensfähigkeit bedeuten, nicht Komfort.

VII. Governance: Wer schaltet was wann?

Technik ohne Verantwortungslogik ist wertlos. Eine kritische Zelle braucht vorab definierte Rollen und eine klare Entscheidungslogik:

Rollen und Zuständigkeiten

- **Netzbetreiber:** Netzschutz, Freischaltung/Trennung, sichere Wiederankopplung
- **Betreiber kritische Zelle:** Lastklassen-Plan, interne Umschaltung, Betrieb der Notversorgung
- **Kommune/Katastrophenschutz:** Lagekoordination, Priorisierung zwischen Zellen, Ressourcenlenkung

- **THW/Einsatzkräfte:** Mobile Einspeisung, Logistik, Führungsfähigkeit vor Ort

Entscheidungs- und Befehlskette

Auslösung Inselbetrieb: Wird durch den Netzbetreiber (technische Notwendigkeit) oder die Katastrophenschutzbehörde (Lageentscheidung) nach vordefinierter Betriebsanweisung ausgelöst. Die Edge-Intelligenz führt dann autonom den Übergang durch.

Priorisierung zwischen Zellen: Kommune/Katastrophenschutz entscheidet auf Basis des Lagebildes, welche Zellen Vorrang erhalten. Entscheidung basiert auf Lastklassen (Life Safety > Medical Ops > Grundbetrieb) und verfügbaren Ressourcen.

Wiederankopplung: Erfolgt koordiniert zwischen Netzbetreiber (Netzstabilität) und Edge (Bereitschaft zur Synchronisation). Ohne nachgewiesene Übung keine Freigabe.

Haftung/Regelwerk: Betrieb erfolgt nach vordefinierter Betriebsanweisung (Schaltlisten, Lastklassen, Übungsprotokolle). Die rechtliche Grundlage bilden Katastrophenschutzgesetze der Länder sowie die Betreiberpflichten nach EnWG/IT-SiG.

Übungspflicht: Blackstart- und Inselnetz-Tests sind der Kern glaubwürdiger Governance. Resilienz muss geübt werden, nicht nur geplant.

VIII. Ausblick: KI in der Krisensteuerung

Die Rolle von KI-Systemen in der Krisensteuerung – von individualisierter Krisenkommunikation bis zur Ressourcenkoordination und Lagebildverdichtung – behandeln wir in einem separaten Beitrag.

IX. Fazit: Nationale Sicherheitsarchitektur

Resilienz im 21. Jahrhundert bedeutet: Versorgungssysteme können in funktionsfähigen Zellen weiteratmen, wenn das Zentrum schweigt. Nicht die Leitung schützen, sondern die Funktion erhalten. Dezentral befähigen, statt zentral zu hoffen.

Dazu braucht es drei Dinge:

- **Zellulare Technik:** Inselnetzfähigkeit + Schnittstellen + mobile Energie + thermische Trägheit
- **Gesicherte Steuerung:** Trust-Infrastruktur für dezentrale Autorität
- **Geübte Governance:** Übungen + Verantwortlichkeit + dokumentierte Prozesse + klare Befehlsketten

Der Perspektivwechsel ist vollzogen: vom Objektschutz zur funktionalen Resilienz.

Transparenzhinweis: Der Beitrag wurde in co-creation unter Nutzung generativer KI-Systeme (Gemini, ChatGPT, Claude) erarbeitet. Inhaltliche Verantwortung, Einordnung und finale Freigabe liegen bei Miriam Schnürer

Literatur- und Quellenverzeichnis

Strategien, Vorsorge, Preparedness

- Europäische Kommission & Hohe Vertreterin der Union für Außen- und Sicherheitspolitik (2025): Joint Communication to the European Parliament and the Council – Preparedness Union Strategy. JOIN(2025) 130 final, 26.03.2025.
- Myndigheten för samhällsskydd och beredskap (MSB) (2024): Om krisen eller kriget kommer (Haushaltsbroschüre / Vorsorge). Publ.-Nr. (MSB), November 2024.
- Krisinformation.se (o. J., Stand lt. Webseite): Hemberedskap – så klarar du dig i en vecka (Schwedische Krisenvorsorge / 1 Woche).
- 72tuntia.fi (o. J.): 72 tuntia – Varautuminen / 72 hours preparedness (Finnisches Vorsorgekonzept).
- Government Offices of Sweden / Sveriges regering (o. J.): Totalförsvär / Total Defence (Konzept der gekoppelten zivil-militärischen Gesamtverteidigung).

Recht & regulatorische Rahmenwerke

- Europäische Union (2022): Richtlinie (EU) 2022/2555 (NIS2) über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union. ABl. L 333, 27.12.2022.
- Europäische Union (2022): Richtlinie (EU) 2022/2557 (CER) über die Resilienz kritischer Einrichtungen. ABl. L 333, 27.12.2022.
- Bundesrepublik Deutschland (aktuelle Fassung): Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). (Konsolidierte Fassung, „Gesetze im Internet“).
- Bundesrepublik Deutschland (aktuelle Fassung): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV). (Konsolidierte Fassung, „Gesetze im Internet“).

Normen, Standards, technische Regelwerke

- IEC (International Electrotechnical Commission): IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems. (Normenreihe).
- IEC (International Electrotechnical Commission): IEC 61850 – Communication networks and systems for power utility automation.
- IEC (International Electrotechnical Commission): IEC 62351 – Power systems management and associated information exchange – Data and communications security.

- IEC (International Electrotechnical Commission): IEC 62443 – Industrial communication networks – Network and system security. (Normenreihe).
- ISO (International Organization for Standardization) (2019): ISO 22301:2019 – Security and resilience — Business continuity management systems — Requirements.
- ISO (International Organization for Standardization) (2022): ISO 15118-20:2022 – Road vehicles — Vehicle to grid communication interface — Part 20: 2nd generation network and application protocol requirements.
- VDE|FNN (2019): VDE-AR-N 4100 (TAR Niederspannung) – Technische Regeln für den Anschluss von Kundenanlagen an das Niederspannungsnetz.
- VDE|FNN (aktuelle Fassung): VDE-AR-N 4105 – Erzeugungsanlagen am Niederspannungsnetz (Anschluss und Betrieb).
- DIN VDE (2023): DIN VDE V 0100-551-2 (VDE V 0100-551-2):2023-10 – Errichten von Niederspannungsanlagen / Stromerzeugungseinrichtungen; Anforderungen u. a. für Einspeisung/Ersatzstrom (mobile/stationäre Quellen).
- DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik) (2023): Microgrids: Wichtiger Beitrag für mehr Resilienz und Versorgungssicherheit in Energiesystemen. (Einordnung/Überblick, inkl. Bezug zu IEC 61850 / IEC 62351).

Cyber-/Trust-Grundlagen (Kryptographie, PKI, Baseline)

- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023): IT-Grundschutz-Kompendium – Edition 2023.
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2025): BSI TR-02102-1 – Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Version 2025-01, 04.03.2025.
- IETF (2008): RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Projekt-/Framework-Quellen

- Borries, Hans-Walter (2023): Business Continuity Management: Resilienz durch nachhaltiges Krisen- und Notfallmanagement. Kompendium (FIRMITAS / BSKI e. V.).
- Schnürer, Miriam (2025): From Critical Infrastructure to Coupled System Governance – Structure-Space / 6-Layer Framework & Multi-Tier-Logik. (Arbeitsfassung / Manuskript, unveröffentlicht bzw. projektintern, falls nicht publiziert).
- Jensen, Marten (2021): Energielogistik und Sektorenkopplung am GreenTEC Campus – Vision der mobilen Energielogistik. (Unternehmenspublikation / Konzeptpapier).

Fahrzeug-/Batterie-Kapazitäten (Beispielquellen für E-Bus-Abschnitt)

- Daimler Truck (2025): The new NMC4 battery in the Mercedes-Benz eCitaro (Presseinformation; u. a. eCitaro G bis 777 kWh, konfigurationsabhängig). 02.10.2025.
- Electrify-/Branchenpublikation (2025): Solaris Urbino 18 electric – Batteriekapazitäten bis 800 kWh (gross), konfigurationsabhängig (Fachbericht / Branchenquelle).
- eBusTool (o. J., Stand lt. Webseite): Urbino 18 electric – Modellübersicht / technische Eckdaten (bis 800 kWh, konfigurationsabhängig).

Abkürzungs- und Begriffsverzeichnis

- **ABL:** Amtsblatt (EU)
- **BHKW:** Blockheizkraftwerk (Kraft-Wärme-Kopplung)
- **BCM:** Business Continuity Management
- **Blackstart (Schwarzstart):** Fähigkeit, Erzeugung/Teilnetz ohne externes Netz wieder hochzufahren.
- **BSI:** Bundesamt für Sicherheit in der Informationstechnik
- **BSIG:** Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
- **BSI-KritisV:** Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
- **BSKI:** Bundesverband für den Schutz Kritischer Infrastrukturen e. V.
- **CER:** Critical Entities Resilience (EU-Richtlinie 2022/2557)
- **Common-Mode-Failure:** Gleichursachen-Ausfall; Redundanz versagt, weil Haupt- und Reservepfad durch denselben Auslöser betroffen sind (z. B. räumliche Bündelung).
- **Docking Port:** Standardisierte, normkonforme Einspeise-/Anschlussstelle für mobile Energiequellen (Aggregate, Batteriecontainer, E-Flotten) inkl. Schutz-/Umschaltkonzept.
- **DKE:** Deutsche Kommission Elektrotechnik Elektronik Informationstechnik (DIN und VDE)
- **DIN:** Deutsches Institut für Normung
- **Edge:** Lokale Ebene (Gebäude/Quartier) mit autonomer Notbetriebslogik (offlinefähig, deterministisch).
- **Grid-forming / netzbildend:** Wechselrichter/Erzeuger, die Spannung/Frequenz aktiv vorgeben (relevant für stabilen Inselbetrieb).
- **Hub:** Regionale Koordinationsebene zwischen Zentral (Backbone) und Edge (z. B. Lagekoordination, Ressourcenlenkung).
- **IEC:** International Electrotechnical Commission
- **Inselnetzfähigkeit (Microgrid-Fähigkeit):** Fähigkeit eines Teilnetzes, sich vom Verbundnetz zu trennen und Spannung/Frequenz lokal stabil zu halten.
- **ISO:** International Organization for Standardization
- **KI:** Künstliche Intelligenz
- **KRITIS:** Kritische Infrastrukturen (z. B. Energie, Wasser, Gesundheit, IT/TK)
- **Layer (6-Layer-Modell / WAS):** Funktionale Schichten: Geo, Infrastructure, Control & Logic, Data, Process, Governance.
- **LoRaWAN:** Long Range Wide Area Network (stromsparende Funktechnik für Telemetrie/Statusdaten)
- **NIS2:** EU-Richtlinie 2022/2555 (Cybersicherheitsniveau / Pflichtenregime)
- **ÖPNV:** Öffentlicher Personennahverkehr
- **PCS:** Power Conversion System (Leistungselektronik/Wechselrichter)
- **PKI:** Public Key Infrastructure (Zertifikate/Schlüssel/Signaturen zur Authentisierung und Befehlsfreigabe)
- **Safety-Controller:** Deterministische Steuerung (z. B. Sicherheits-SPS/Controller) zur sicheren Umschaltung (Normalbetrieb ↔ Inselbetrieb ↔ Wiederankopplung) und zur Begrenzung von Last-/Schaltspitzen.
- **State-Sync / Snapshots:** Lokales Vorhalten kritischer Betriebsdaten/Lastklassenprofile am Edge (z. B. als vorab geladene Zustandsabbilder), um bei Trennung sofort handlungsfähig zu sein.
- **THW:** Technisches Hilfswerk

- **Tier (Multi-Tier-Logik / WO):** Autoritäts- und Betriebsräume: Zentral (Backbone) → Regional (Hub) → Lokal (Edge).
- **TPM:** Trusted Platform Module (Hardware-Sicherheitsbaustein für Schlüssel/Attestierung/Device-Trust)
- **Trust Plane:** Sicherheits- und Identitätsebene für legitime Schalt-/Steuerbefehle (Signatures, Geräteattestierung, Schlüsselmanagement, Audit-Trail).
- **V2G:** Vehicle-to-Grid (bidirektionales Laden/Einspeisung ins Netz)
- **V2X:** Vehicle-to-Everything (Kommunikation Fahrzeug ↔ Infrastruktur/Netz/IT-Systeme)
- **VDE / VDE|FNN:** Verband der Elektrotechnik Elektronik Informationstechnik e. V. / Forum Netztechnik/Netzbetrieb im VDE
- **WLAN-Mesh:** Vermashtes lokales Funknetz zur Notkommunikation/Telemetrie (Multi-Hop)