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.

Revision #1
Created 21 November 2025 14:11:15 by Thorsten Zoerner
Updated 21 November 2025 14:11:15 by Thorsten Zoerner