

Warum die Datenprozesse für Smart Meter bzw. intelligente Messsysteme (iMSys) in Deutschland kompliziert und teuer sind

TL;DR

- **Akteursvielfalt:** 800 Netzbetreiber, über 1.000 Lieferanten, hunderte Messstellenbetreiber. Jeder Prozess muss hochstandardisiert sein, pragmatische Lösungen sind unmöglich.
- **Bilaterale Marktkommunikation:** Jeder tauscht mit jedem Daten aus, eine zentrale Plattform (wie die DCC in UK) fehlt. Jeder Marktteilnehmer muss eine eigene, halbjährlich zu aktualisierende IT-Infrastruktur vorhalten.
- **Vielgliedrige IT-Landschaft:** Jeder Messstellenbetreiber muss ein Dutzend IT-Systeme verschiedener Anbieter betreiben, getrieben ist das auch durch die regulatorischen Anforderungen im Messtellenbetriebsgesetz (u.a. Standard- und Zusatzleistungen)
- **BSI-Sicherheitsarchitektur:** Legt nochmal eine zusätzliche Komplexitätsebene über die Prozesse. Die Nutzung des Gateway-Administrators (GWA) ist bei jedem Vorgang am Gerät ein zwingender Zwischenschritt.
- **Smart Meter light** löst nicht alle Probleme, sorgt aber für Vereinfachungen in Punkten BSI-Sicherheitsarchitektur (fällt weg) und vielgliedrige IT-Landschaft (weniger Funktionen und Anforderungen)

1. Die Akteursvielfalt macht pragmatische Lösungen unmöglich

Deutschland hat eine im internationalen Vergleich einzigartig hohe Akteursvielfalt im Strommarkt. An einem Zählpunkt hängen mindestens fünf Parteien mit gesetzlich definierten Datenansprüchen (§§ 60 ff. MsbG): Anschlussnutzer, Lieferant, Verteilnetzbetreiber, Messstellenbetreiber und Übertragungsnetzbetreiber, dazu gegebenenfalls Direktvermarkter oder Energieserviceanbieter. Der Datenaustausch findet zwischen rund 800 Netzbetreibern, über 1.000 Lieferanten und hunderten Messstellenbetreibern statt.

Die Folge: Jeder Prozess muss hochstandardisiert sein, damit er zwischen allen denkbaren Kombinationen von Marktpartnern diskriminierungsfrei und massentauglich funktioniert. Workarounds und pragmatische bilaterale Lösungen, wie sie zwischen zwei Unternehmen üblich wären, sind in dieser Konstellation nicht möglich. Was nicht im Standard abgebildet ist, funktioniert im Markt nicht. Und jede Änderung am Standard muss von allen Akteuren umgesetzt werden, bis sie flächendeckend funktioniert

In Frankreich und Italien gibt es diese Akteursvielfalt nicht. Dort ist der eine bzw. größte Verteilnetzbetreiber (Enedis bzw. e-distribuzione) für den Rollout verantwortlich; der Zähler gehört zum Netzanschluss, der Verteilnetzbetreiber sammelt die Daten ein, verarbeitet sie und verteilt sie an Lieferanten weiter. Wettbewerb und Wechselprozesse gibt es nicht.

In Großbritannien läuft es anders: Dort gibt es Wettbewerb im Messwesen, für den Einbau sind

die Stromlieferanten (und nicht die Netzbetreiber) verantwortlich. Die Akteursvielfalt ist trotzdem deutlich geringer als in Deutschland; die meisten Einbauten wickeln die acht großen Versorger ab, alle Marktteilnehmer können außerdem auf die zentrale Datenplattform DCC zugreifen.

2. Daten werden bilateral ausgetauscht (Marktkommunikation), jeder Marktteilnehmer muss eine up-to-date IT-Infrastruktur vorhalten

Der standardisierte Datenaustausch zwischen den Marktteilnehmern heißt [Marktkommunikation \(MaKo\)](#). Sie funktioniert bilateral: Jeder Marktpartner tauscht automatisiert elektronische Nachrichten nach standardisierten Formaten und Codes direkt mit jedem anderen aus. Der Austausch erfolgt über eine automatisierte E-Mail-Infrastruktur (im sog. EDIFACT-Format), eine zentrale Datenplattform gibt es nicht.

Für jeden Messstellen- und Verteilnetzbetreiber bedeutet das: Er muss eine eigene IT-Infrastruktur für die Marktkommunikation aufbauen oder sich einen spezialisierten IT-Dienstleister suchen, halbjährliche Aktualisierungen (sog. Formatanpassung) umsetzen und mit seinen Gegenparteien testen. Dafür braucht es hochspezialisierte IT-Dienstleister und viele hochspezialisierte Mitarbeiter

In der Praxis beherrschen viele Marktpartner vor allem die neuen MaKo-Prozesse rund um Smart Meter nach wie vor nicht zuverlässig. Fehlerhafte Stammdaten, verspätete Rückmeldungen oder fehlerhafte oder nicht existierende (weil noch nicht erarbeitete) Codes führen sofort zu Ausfällen im Datenaustausch, die individuell und manuell geklärt werden müssen. Bei uns ist bei rund 20 Prozent der Smart Meter eine manuelle Klärung notwendig, was enorme Kosten verursacht.

Die wichtigsten Prozessregelwerke innerhalb der MaKo sind die GPKE (Geschäftsprozesse zur Kundenbelieferung mit Elektrizität, u. a. für den Lieferantenwechsel und die Messwertübermittlung an den Lieferanten) und die WiM (Wechselprozesse im Messwesen, u. a. für den Wechsel des Messstellenbetreibers und den Zählertausch). Die Regelwerke und Codes werden von der Branche laufend weiterentwickelt (in den edi@energy-Gremien beim BDEW), von der Bundesnetzagentur verbindlich festgelegt und in der Regel halbjährlich angepasst.

Unter anderem in UK läuft der Datenzugriff über eine zentrale Datenplattform ([DCC, Data Communications Company](#)). Der Regulator Ofgem (vergleichbar mit der Bundesnetzagentur) schreibt den Betrieb der Plattform künftig für sechs Jahre aus, der Betrieb lief bisher über ein IT-Dienstleistungsunternehmen, künftig ist es ein Gemeinschaftsunternehmen der Branche. Eine Anbindung an die Plattform genügt dort für den Austausch mit allen Marktteilnehmern, Marktprozesse müssen nicht von allen Marktteilnehmern vorgehalten und ständig aktualisiert werden

Gelöst werden könnte das Problem grundsätzlich über eine zentrale Datenplattform. Die

Bundesnetzagentur hat mit dem sog. MaBis-Hub für die Bilanzkreisabrechnung Strom einen ersten Schritt in diese Richtung gemacht, allerdings gestaltet sich die Umsetzung komplex und verzögert sich (wegen der Akteursvielfalt).

3. U.A. die regulatorischen Anforderungen haben bei jedem Messstellenbetreiber eine vielgliedrige IT-Systemlandschaft entstehen lassen, in der jede Änderung durch alle Systeme wandern muss

Ein Messstellenbetreiber betreibt für den Smart-Meter-Rollout nicht ein oder zwei IT-Systeme, sondern eine komplexe, historisch gewachsene IT- und Prozesslandschaft.

Zum Smart-Meter-Betrieb gehören unter anderem ERP (Enterprise Resource Planning, das zentrale kaufmännische Unternehmenssystem, in dem die Geschäftsprozesse zusammenlaufen) und Abrechnung, Vertrags- und Stammdatenverwaltung, Marktkommunikation, Geräteverwaltung, Workforce-Management für die Monteure, Gateway-Administration, Messdatenmanagement, die Überwachung der Funkanbindung, Visualisierungsportale für Kunden und durch den Steuerungsrollout künftig auch das CLS-Management für Schalt- und Steuerbefehle.

Diese Funktionen werden häufig durch Systeme unterschiedlicher IT-Dienstleister abgedeckt, im ERP-Umfeld beispielsweise SAP, Schleupen, Wilken oder SIV, im Umfeld von Gateway-Administration, Messdatenmanagement und CLS unter anderem Robotron, BTC oder TREMONDI.

Die Vielgliederigkeit ist auch eine Folge der regulatorischen Anforderungen. Jeder Tarifierungsfall (TAF) – also die im Gerät hinterlegte Vorgabe, welche Daten und Werte in welchem Takt und an wen übermittelt werden – muss in den Systemen abgebildet werden, vom einfachen Jahresverbrauch bis zur viertelstündlichen Übermittlung für dynamische Tarife. Das MsbG definiert dazu verpflichtende Standard- und Zusatzleistungen (§§ 34, 35 MsbG), die jeweils eigene Prozesse erzwingen: etwa den Einbau auf Kundenwunsch innerhalb von vier Monaten, die Bündelung und Aufteilung der Preisobergrenzen in der Abrechnung oder die Pflicht, Kunden ihre Messwerte über ein Portal zu visualisieren (§§ 61, 62 MsbG). Mit der Steuerung nach § 14a EnWG und § 9 EEG kommt eine weitere Systemebene hinzu. Jede dieser Pflichten muss von den Softwareherstellern entwickelt, vom Messstellenbetreiber integriert und im Betrieb beherrscht werden, unabhängig davon, wie viele Kunden die jeweilige Leistung tatsächlich nachfragen.

Eine regulatorische Änderung betrifft selten nur einen isolierten Prozess. Wird ein Datenobjekt, eine Codeliste, ein Tarifierungsfall oder eine Prozesslogik geändert, kann das Auswirkungen auf Stammdaten, Marktkommunikation, Geräteverwaltung, Messdatenmanagement, Abrechnung, Montageprozesse sowie GWA- und CLS-Systeme haben. Die Anpassungen müssen zunächst durch die unterschiedlichen Softwarehersteller umgesetzt, anschließend in die jeweilige Systemlandschaft des Messstellenbetreibers integriert

und schließlich Ende zu Ende getestet werden. Selbst kleine Änderungen können daher zahlreiche Folgeprozesse und Schnittstellen betreffen. Das erklärt, warum die halbjährlichen Formatanpassungen und kurzfristige Gesetzesänderungen die Branche so stark binden.

Die konkrete Architektur und die Kombination der Anbieter unterscheiden sich von Messstellenbetreiber zu Messstellenbetreiber. Auch bei standardisierten Marktprozessen bleiben daher unternehmensindividuelle Schnittstellen, Integrationen und teilweise Sonderlösungen bestehen. Daraus resultiert zugleich eine erhebliche Abhängigkeit von den jeweiligen Softwarelieferanten und deren Releaseplanung. Zwischen den Systemen existieren nur wenige einheitliche Schnittstellen, Automatisierung ist stets ein unternehmensindividuelles Unterfangen, ein stabiler, eingespielter Systembetrieb wird so seit Jahren nicht erreicht.

Hier liegt auch die Antwort auf die Frage, weshalb nicht einfach eine Excel-Liste

ausreicht: Eine Excel- oder CSV-Liste kann in einer Pilotierung oder als manueller Workaround einzelne Daten zwischen zwei Systemen transportieren. Sie bildet aber keinen massenfähigen Ende-zu-Ende-Prozess ab. Dafür müssen Stammdaten, Berechtigungen, Prozessstatus, Rückmeldungen, Fristen und Fehlerfälle über mehrere Systeme und Markttrollen hinweg konsistent verarbeitet werden. Der Steuerungsrollout illustriert genau diesen Unterschied: Für einen technischen Durchstich mit kleinen Stückzahlen lassen sich Stammdaten zwischen den Systemen noch über CSV-Workarounds austauschen. Für einen Massenprozess braucht es dagegen vollständige Datenmodelle, automatisierte Schnittstellen und eine durchgängige Orchestrierung der gesamten Prozesskette, vom Netzbetreiber-Portal über ERP, Marktkommunikation, Gateway-Administration und Messdatenmanagement bis zum Gerät in der Kundenanlage.

4. Die BSI-Sicherheitsarchitektur legt eine zusätzliche, aufwändige Schicht über die IT-Prozesslandschaft

Innerhalb dieser ohnehin komplexen Gesamtarchitektur bildet die BSI-Sicherheitsarchitektur eine zusätzliche, komplexe Schicht.

Nur ein [vom BSI zertifizierter Gateway-Administrator \(GWA\)](#) darf Einstellungen am Sicherheitsmodul des Smart Meter Gateway (also dem Kommunikationsmodul des iMSys) vornehmen. Die Rolle GWA ist der verantwortliche technische Betreiber des Gateways, entweder ist das der Messstellenbetreiber selbst (nach BSI-Zertifizierung) oder ein von ihm beauftragtes, nach BSI-Vorgaben zertifiziertes Unternehmen.

Der GWA nimmt jedes Gateway einzeln in Betrieb, verwaltet vom BSI vorgeschriebenen Sicherheitszertifikate für jedes Gerät und jeden Datenempfänger, spielt Updates ein und stellt jede Änderung neu ein.

Für den Messstellenbetreiber wird die Geräteverwaltung damit noch teurer und komplizierter. Er muss entweder selbst die aufwändige BSI-Zertifizierung durchlaufen oder die GWA-Funktion bei einem der zertifizierten Dienstleister einkaufen. Wird die Funktion ausgelagert, gibt ER die Entscheidungsgewalt über zentrale Betriebsprozesse an den Dienstleister ab und kann bei

Störungen oder Änderungen nicht selbst eingreifen.

Jeder Vorgang am Gerät, von der Inbetriebnahme bis zur kleinsten Änderung der Datenflüsse, läuft über den Gateway-Administrator und wird zu einer Prozesskette mit einem Dritten, dessen Systeme mit den Systemen des Messstellenbetreibers fehlerfrei zusammenspielen müssen. Oft tun sie das nicht, wodurch wiederum manuelle Klärungen notwendig sind.

Gleichzeitig sind die GWA-Systeme nicht einfach so interoperabel. Am Umzug eines Smart-Meter-Gateways von einem GWA zum nächsten GWA (z.B. wenn ein GWA Fehler macht) sind bis zu zehn Stakeholder involviert. So muss etwa der Sim-Karten-Provider des GWA-Betreiber eingebunden werden. Der Prozess ist damit so aufwändig, dass er sich für einzelne Geräte nicht lohnt. In der Praxis werden die Intelligenten Messsysteme deshalb oft physisch ausgebaut, wenn ein GWA-Wechsel notwendig wird oder auch wenn der Kunde seinen Messstellenbetreiber wechselt (was er rein rechtlich darf).

Dazu kommt, dass das BSI für Gateways Sicherheitszertifikate vergibt (für Verschlüsselung, Signatur, gesicherte Verbindung), die alle zwei Jahre erneuert werden müssen. Sonst verliert das Gateway die Fähigkeit zur sicheren Kommunikation und ist praktisch Elektroschrott. Daraus ergibt sich auch nach einigen Jahren ein erheblicher dauerhafter Anpassungs- und Infrastrukturaufwand für GWA und Messstellenbetreiber.

Abschließend: Ein Smart Meter light kann nicht alle diese Probleme lösen. Aber das Konzept würde aber auf die BSI-Sicherheitsarchitektur und die Gateway-Administration (die ohnehin auf das Sicherheitsniveau eines Geräts abzielt, über das Wärmepumpen, Wallboxen und PV-Anlagen gesteuert werden können) verzichten. Auch der im Messstellenbetriebsgesetz vorgeschriebene Funktionsumfang würde beim Smart Meter light deutlich geringer ausfallen, wodurch weniger IT-Prozesse und IT-Dienstleister für den Betrieb der Geräte notwendig sind. All das spart Kosten (zusätzlich zu geringeren Hardware-Kosten).

Der Messstellenbetrieb ist reformbedürftig, aber gleichzeitig fragil. Deshalb müssen bestehende Prozesse, soweit möglich, weiter genutzt werden. Hau-Ruck-Änderungen und neue Vorgaben würden Investitionen gefährden und dem Rollout schaden, statt ihn zu beschleunigen. Ein Smart Meter Light wäre richtig ausgestaltet und ohne zusätzliche Vorgaben ein chirurgischer Eingriff, der die Komplexität für den Masseneinbau reduziert, ohne das System zu gefährden.