Implementierung & Architektur

Der Paradigmenwechsel in der Systemarchitektur: Von statischen Punkt-zu-Punkt-APIs hin zu aktiven, prozessgesteuerten KI-Agentennetzwerken. Referenzarchitekturen und Best Practices für die sichere Integration in KRITIS-Umgebungen.

- Ausblick: Energiesystemanalyse jenseits der Physik
- Wissenschaftliche Standardisierung und Data Provenance
- Das Cernion Cookbook (Best Practices in Code)

Ausblick: Energiesystemanalyse jenseits der Physik

Die deutsche Energiesystemanalyse hat sich über Jahrzehnte als ingenieurwissenschaftliche Disziplin verstanden. Ihre Werkzeuge sind Lastflussberechnungen, Netzausbauoptimierungen und stochastische Einspeisemodelle. Ihre Sprache ist die Sprache der Physik: Impedanzen, Spannungsbänder, (n-1)-Sicherheit. Ihre Ergebnisse fließen in Netzentwicklungspläne, NOVA-Prüfungen und Investitionsentscheidungen über Kupfer und Transformatoren.

Diese Perspektive war richtig und notwendig. Sie reicht aber nicht mehr aus.

Die vorangegangenen Kapitel dieser Serie haben gezeigt, dass der operative Engpass der Energiewende nicht in der physikalischen Netzplanung liegt, sondern in der **administrativen Prozesssteuerung**: in der Asynchronität zwischen Marktstammdatenregister und GIS, zwischen BTR-Zuordnung und EDIFACT-Meldung, zwischen Prognoseprofil und tatsächlicher Anlagenkapazität. Diese Prozess-Asynchronität erzeugt Reibungsverluste, die sich nicht durch Netzausbau beseitigen lassen — weil sie nicht physischer, sondern informationeller Natur sind. Ein neuer Transformator löst kein Problem, das in einer fehlenden MeLo-Zuordnung liegt.

Forschungsnetzwerk Energiesystemanalyse: Themengruppe 4

Das **Forschungsnetzwerk Energiesystemanalyse (FNE)** hat diesen Paradigmenwechsel erkannt. Für den Forschungszyklus 2026/2027 wurde die **Themengruppe 4: „Automatisierte Konsistenzprüfung und agentische Prozesssteuerung im Assetmanagement (Agentic Asset-MDM)"** unter der Leitung der **STROMDAO GmbH** eingerichtet. Die Themengruppe adressiert die systematische Lücke zwischen der physikalischen Netzmodellierung und der administrativen Datenintegrität, die den operativen Netzbetrieb heute stärker limitiert als die installierte Leitungskapazität.

Die Fokusthemen der Themengruppe umfassen drei Forschungsfelder. Erstens die **Komplexitätsreduktion im Verteilnetzbetrieb**: Wie lassen sich die kombinatorischen Abhängigkeiten zwischen vier bis fünf Quellsystemen (MaStR, GIS, ERP, Leitsystem, Prognoseplattform) so orchestrieren, dass der Sachbearbeiter nicht mehr als Integrator zwischen

asynchronen Datenständen fungieren muss? Zweitens die **Integration öffentlicher Stromnetzdaten**: Welche Rolle spielt das Marktstammdatenregister als autoritative Referenz für Netz-Assets, und wie lassen sich seine Datenqualitätsprobleme (Phantom-Anlagen, fehlende Stilllegungen, Netzgebiets-Fehlzuordnungen) systematisch adressieren? Drittens die **autonomen Validierungspipelines**: Wie müssen Software-Agenten architektonisch beschaffen sein, damit sie den Stammdaten-Zustand eines Netzgebiets nicht nur prüfen, sondern heilen können — deterministisch, auditierbar und mit definierten Eskalationsstufen?

STROMDAO: Offene Dateninfrastruktur für die Energiewende

Die STROMDAO GmbH hat das Framework Agentic Asset-MDM nicht als akademische Übung entwickelt, sondern aus der operativen Erfahrung im Verteilnetzbetrieb. Als Unternehmen, das seit 2017 an der Schnittstelle von Energiedateninfrastruktur und regulatorischer Praxis arbeitet, hat STROMDAO die Lücke zwischen der regulatorischen Pflicht (§ 8 EnWG, Redispatch 2.0, EWK-Monitoring) und der technischen Machbarkeit im kommunalen Verteilnetz systematisch analysiert und in eine formalisierte Methodik überführt — dokumentiert in dieser Serie auf currently.io.

Die Methodik ist offen. Die wissenschaftlichen Fragestellungen, die sie aufwirft, sind es ebenfalls. Die Themengruppe 4 im FNE ist der institutionelle Rahmen, in dem diese Fragen mit Netzbetreibern, Forschungseinrichtungen und Regulierungsbehörden diskutiert werden.

Einladung

Das **FNE-Jahrestreffen 2026** wird die Themengruppe 4 erstmals im Auditorium vorstellen. Verteilnetzbetreiber, die den Diskurs über administrative Datenintegrität als Engpass der Energiewende mitgestalten wollen, sind eingeladen, sich an der Themengruppe zu beteiligen.

Wer die Ergebnisse nicht abwarten, sondern die Methodik heute in die operative Praxis umsetzen möchte, findet mit **Cernion** die schlüsselfertige Implementierung — autonome Validierungsagenten für Verteilnetzbetreiber, entwickelt von STROMDAO, getestet im Realbetrieb.

Wissenschaftliche Standardisierung und Data Provenance

Die Energiewirtschaft zählt zu den kritischen Infrastrukturen (KRITIS). Mit zunehmender Dezentralisierung stoßen traditionelle, silobasierte Stammdaten-Systeme an ihre Grenzen. Die Einführung von Künstlicher Intelligenz – insbesondere Agentic AI – zur automatisierten Konsistenzprüfung von Anlagenstammdaten erfordert ein neues Maß an Auditierbarkeit und Interoperabilität. Die Lösung für das sogenannte Vendor-Lock-in-Problem proprietärer Software-Silos liegt in der konsequenten Adaption wissenschaftlicher Datenstandards.

Cernion, als Referenzimplementierung für das Agentic Asset Master Data Management (a²mdm), löst diese Herausforderung architektonisch durch den **FAIR Data Layer** (eingeführt in v0.11 und finalisiert in v0.12).

Dieses Kapitel beleuchtet die technische Implementierung der FAIR-Prinzipien (Findable, Accessible, Interoperable, Reusable), die Integration der Open Energy Ontology (OEO) und die Sicherstellung von Data Provenance gemäß den Vorgaben des EU AI Acts für Hochrisiko-Systeme.

---

1. Vermeidung von Vendor-Lock-ins durch die Open Energy Ontology (OEO)

Ein zentrales Problem der Datenintegration bei Verteilnetzbetreibern ist das Fehlen eines gemeinsamen, maschinenlesbaren Vokabulars. Cernion begegnet diesem Problem durch eine native, statische Mapping-Schicht auf die **Open Energy Ontology (OEO)**, dem Standard-Vokabular der Nationalen Forschungsdateninfrastruktur (NFDI4Energy).

Technische Umsetzung (`oeo-mappings.js` & `sync-oeo.js`):
Cernion verzichtet bewusst auf einen ressourcenintensiven, vollumfänglichen Knowledge Graph (SPARQL-Endpoint) zur Laufzeit. Stattdessen zieht ein dediziertes Entwickler-Skript (`npm run sync:oeo`) die aktuellste OEO-ETD-CSV von GitHub und kompiliert daraus ein hochperformantes, statisches Lookup-Modul (`src/oeo-mappings.js`).

Dieses Modul umfasst ca. 150 kuratierte Mappings, die präzise auf die Anforderungen im Assetmanagement (z.B. Marktstammdatenregister / MaStR) zugeschnitten sind. Beispielsweise wird das MaStR-Feld `Lage` bei Windkraftanlagen nicht einfach als Text verarbeitet, sondern semantisch

differenziert in `wind-onshore` (OEO_00000446) und `wind-offshore`.

Semantische Anreicherung der KI (Classifier Enrichment):
Ein besonderer Architektureingriff liegt in der Nutzung der deutschen OEO-Labels (`labelDe`, z.B. „Umspannwerk“ oder „Solaranlage“). Diese Begriffe werden automatisiert in den Keyword-Pool der Cernion-Klassifizierungs-KI (Classifier) überführt. Dies boostet die heuristische Erkennungsrate bei unstrukturierten, deutschsprachigen Daten-Uploads von Netzbetreibern erheblich, ohne den eigentlichen Scoring-Algorithmus anpassen zu müssen.

OpenAPI-Annotationen:
Alle REST-Endpunkte (über 45 Actions in 7 Domänen wie `grid-operations` oder `energy-market`) sind via OpenAPI mit einer `x-oeo-class`-Erweiterung annotiert. Zusätzlich wird ein JSON-LD Endpunkt (`GET /api/datapoints/oeo-context`) bereitgestellt, der das Mapping von internen Cernion-Feldern auf OEO-IRIs als `@context`-Dokument ausliefert.

---

2. Data Provenance & KRITIS-Compliance (Der EU AI Act in der Architektur)

Systeme, die als Sicherheitskomponenten in der Verwaltung kritischer Infrastrukturen eingesetzt werden, unterliegen künftig den strengen Vorgaben des EU AI Acts für Hochrisiko-KI-Systeme (Art. 10, 12, 15). Die Kernanforderung lautet: **Data Provenance**. Es muss jederzeit kryptografisch nachweisbar sein, auf welcher Datengrundlage (Quellen, Lizenzen, Zeitstempel) ein KI-Agent eine Entscheidung (z.B. eine automatisierte Stammdaten-Korrektur) getroffen hat, um “KI-Halluzinationen” auszuschließen.

Die In-Memory-Edge-Architektur (PouchDB):
Cernion garantiert KRITIS-Compliance durch eine strikte In-Memory-Policy am Edge. Sensible Netztopologie- oder Assetdaten (z.B. im `Datapoint Layer`) verbleiben in der lokalen PouchDB-Instanz des Betreibers und werden nicht unmaskiert an externe Cloud-LLMs gesendet. Die Agenten operieren primär auf Basis der anonymisierten OEO-IRIs.

Der OEMetadata v2.0 Exporter (`oemetadata.service.js`):
Das Herzstück der Provenance-Sicherung ist der OEMetadata-Exporter (eingeführt in v0.11, strikt validiert in v0.12). Jeder verwaltete Cernion-Datenpunkt erzeugt auf Anfrage ein JSON, das exakt dem offiziellen `schema.json` v2.0 des OEMetadata-Projekts entspricht.

Der Exporter extrahiert dynamisch:

- **Temporal & Spatial Data:** Zeitreihen-Begrenzungen und Georeferenzierungen (Bounding Boxen) basierend auf den abgerufenen Datensätzen (z.B. das Netzgebiet „Ludwigshafen“).
- **Sources & Licenses:** Ein Cernion-Agent dokumentiert automatisch in den Metadaten, welche Microservices er abgefragt hat (`sources`). Das System mappt diese auf die korrekten Quell-Lizenzen (z.B. `DL-DE/BY-2.0` für das MaStR oder `CC-BY-4.0` für ENTSO-E).

- **Kryptografischer Hash:** Jeder Export beinhaltet einen kryptografischen Hash (z.B. SHA-256) der rohen Quelldaten zum Zeitpunkt der Agenten-Analyse, was die Auditierbarkeit für den Netzbetreiber rechtssicher macht.

Um sicherzustellen, dass keine invaliden Metadaten ausgeliefert werden, lädt das System während des Builds (`npm run sync:oemetadata`) das offizielle JSON-Schema von der Open Energy Platform herunter. Jede REST-Anfrage (`GET /api/datapoints/:name/oemetadata?validate=true`) wird zur Laufzeit via `ajv` validiert.

---

3. Orchestrierung über Systemgrenzen: Der OEP-Connector

Um KI-Agenten im Assetmanagement wirklich proaktiv handeln zu lassen, müssen sie die lokale Sicht (das eigene Netzgebiet) mit globalen Entwicklungen abgleichen können. Cernion v0.12 führt hierfür einen dedizierten, Read-Only-Connector (`oep.service.js`) zur **Open Energy Platform (OEP)** ein.

Dieser Microservice ermöglicht es dem Agent-Planner, komplexe Fragestellungen in mehrstufige Pläne (Steps) zu zerlegen.
Ein Prompt wie: *“Vergleiche die installierte PV-Leistung bei den TWL Netzen mit dem Netzentwicklungsplan-Szenario (NEP) 2035”* triggert nun folgende automatisierte Kette:

1. Der Agent fragt den lokalen Cernion-Service (`assets.solar`) für das MaStR-Netzgebiet ab.
2. Der Agent nutzt den OEP-Connector (`oep.query`), um das öffentliche NEP-Szenario direkt aus der Datenbank der nationalen Forschungsinfrastruktur zu ziehen.
3. Das LLM (als Reasoning-Layer) interpretiert das Delta lokal und speichert das Ergebnis als validierten Datenpunkt zurück in die PouchDB.

Um die Latenz bei Agenten-Entscheidungen gering zu halten, werden die OEP-Tabellenmetadaten in Cernion im RAM gecacht (TTL von 24h), während die eigentlichen Tabellendaten aus Datenschutzgründen lediglich durch den Speicher fließen (Pass-through).

---

4. Datapoint Scheduling: Kontinuierliche Datenhygiene

Für den operativen Betrieb eines Stadtwerks reicht ein manueller Aktualisierungs-Trigger nicht aus. KI-Agenten können nur dann belastbare Konsistenzprüfungen durchführen, wenn das Daten-Fundament (“Datapoint Layer”) stets aktuell ist.

Mit v0.12 implementiert Cernion ein lokales Interval-Scheduling (`strategy: "interval"`). Der `datapoint.service.js` prüft kontinuierlich (z.B. in einem 60-Sekunden-Tick), ob Datenpunkte veraltet sind. So kann beispielsweise eine “Tägliche Portfolio-Inventur (PV, Wind, Speicher)” konfiguriert werden (`intervalMinutes: 1440`). Ist ein Datenpunkt veraltet, markiert der interne Health-Endpoint diesen als `stale` und triggert autonom einen Refresh.

(Dieser Mechanismus ist essentiell für die Vorbereitung auf Cernion v0.14+, in dem autonome Validierungsagenten kontinuierlich und unbeaufsichtigt auf der Datapoint-Schicht nach Fehlern in der Marktkommunikation oder dem MaStR suchen werden).

Investitionssicherheit durch FAIR Data

Mit der Architektur des FAIR Data Layers positioniert sich Cernion als Referenzimplementierung für das Agentic Asset-MDM. Kein anderer kommerzieller Energiedaten-Agent erzeugt aktuell vollautomatisch OEMetadata-konforme Exporte inkl. OEO-Annotationen und Data-Provenance-Hashes. Für Stadtwerke bedeutet dies: Investitionssicherheit (kein Vendor-Lock-in), lückenlose Nachvollziehbarkeit für Audits (EU AI Act) und sofortige Interoperabilität mit der nationalen Energieforschungslandschaft.

Das Cernion Cookbook (Best Practices in Code)

Der Paradigmenwechsel von starren ETL-Pipelines hin zu Agentic Asset-MDM (A²MDM) erfordert in der KRITIS-Praxis konkrete, validierbare Implementierungen. Um die Lücke zwischen theoretischem Framework und operativem Systemaufbau zu schließen, bündelt das **Cernion Cookbook** Referenzimplementierungen ("Rezepte") in Code.

Diese Rezepte demonstrieren, wie die Cernion Energy Tools (als A²MDM Plattform) komplexe Herausforderungen der Energiewirtschaft autonom über Knowledge Graphs auflösen.

Cernion Energy Tools im Kommunikationsnetz

Cernion Energy Tools (CET) bündeln Energie-, Netz-, Markt- und Betreiberkontext zu prüfbaren Arbeitslagen. Im Cernion Capability Hub sind Datenquellen, REST/OpenAPI, MCP, KI-Agenten, Portfolio-Backtests, kommunale Lagebilder, Workbench- und Reportpfade public-safe beschrieben. corrently.io ergänzt diesen Produktkontext mit Praxis-, Open-Source- und Energiedatenbeispielen für Entwickler und Integratoren.

Nächste Einstiege: Cernion Themencluster für die Such- und Fachstruktur, Verteilnetzbetreiber Software für die Produkt-/Arbeitslagen-Einordnung, Stadtwerke Prozessautomatisierung für kontrollierte Fachprozess-Entlastung sowie KI für Stadtwerke und Netzbetreiber für evidenzgebundene Assistenz mit HITL-Grenzen.

Rezept #1: Der Automatisierte MaStR-Qualitätsaudit

Eine Kernaufgabe von A²MDM-Agenten (siehe Schritt 1: Bestandsinventur) ist der autonome Quellenabgleich. Die toxische Datenqualität des Marktstammdatenregisters (MaStR) führt regelmäßig zu Phantom-Engpässen in der Zielnetzplanung.

Das `mastr-quality-audit` Rezept implementiert die Heuristik zur Bereinigung:
Anstatt Daten naiv aus dem MaStR in ein GIS-System zu spiegeln, traversiert der Cernion-Agent

das Portfolio kontinuierlich. Er erkennt Inkonsistenzen autonom, beispielsweise wenn der Status "In Planung" zu lange anhält oder Leistungsangaben (z.B. 100 kWp) im Knowledge Graph im Widerspruch zu externen geografischen Kontexten (OpenStreetMap-Gebäudeflächen) stehen. Das Ergebnis ist ein validierter "Trusted State", der als verlässliche Entscheidungsgrundlage für nachgelagerte Prozesse dient.

(Die technische Umsetzung und die API-Endpunkte für dieses Audit sind über die Cernion Timeline dokumentiert).

Rezept #2: Die End-to-End Pipeline für Energy Sharing (§42c EnWG)

Transaktionale Sicherheit ist eine der größten Herausforderungen in Netzbetreiber-Architekturen. Wenn kaufmännische Logik auf physikalische Restriktionen trifft, versagen herkömmliche relationale Datenbanken.

Das `energy-sharing-full-pipeline` Rezept demonstriert die architektonische Überlegenheit von Knowledge Graphs bei der Abwicklung des Energy Sharings nach §42c EnWG.
Der Agent bündelt Erzeuger und Verbraucher dynamisch in virtuellen Bilanzkreisen. Kommt es zu einem Netzeingriff (z.B. Redispatch 2.0 / Abregelung einer Community-PV-Anlage), erkennt das System den physikalischen Zustand und löst sofort den kaufmännischen Konflikt: Die Ausfallarbeit wird berechnet, und die Allokationsschlüssel der Community-Mitglieder werden automatisch vorbereitet und prüfbar dokumentiert.

(Weitere Best-Practice-Pipelines, u.a. zur Zielnetzplanung und zu §14a EnWG-Simulationen, werden fortlaufend in das Cookbook integriert).

Cernion Public API Recipes für Entwickler

Für Developer- und LLM-Discovery ist ein public-safe Rezeptpaket zu Cernion Energy Tools vorbereitet. Es beschreibt drei synthetische Einstiegspunkte: OpenAI-kompatible Fachassistenz, Copilot-Intent-Vorbereitung mit pending confirmation und ein Customer-Service-Portal-Widget als Integrationsfixture. Die Beispiele sind für Discovery und Integrationsplanung gedacht, nicht für automatische Freigaben, Billing, Tarifänderungen, MaKo-Ausführung, Gerätesteuerung oder produktive Kundenvorgänge.

- GitHub PR #483: Public API Recipes / LLM Discoverability
- Canonical docs after merge: docs/public-api-recipes.md
- OpenAPI JSON: api.cernion.de/api/openapi.json
- Swagger UI: api.cernion.de/api/docs

Sicherheitsgrenze: Tokens bleiben serverseitig und privat. Öffentlich dokumentierte Requests verwenden synthetische Daten wie `docs-sandbox-slot5`; Live-Tenant-, Kunden-, Vertrags- oder Abrechnungsdaten gehören nicht in Beispiele.