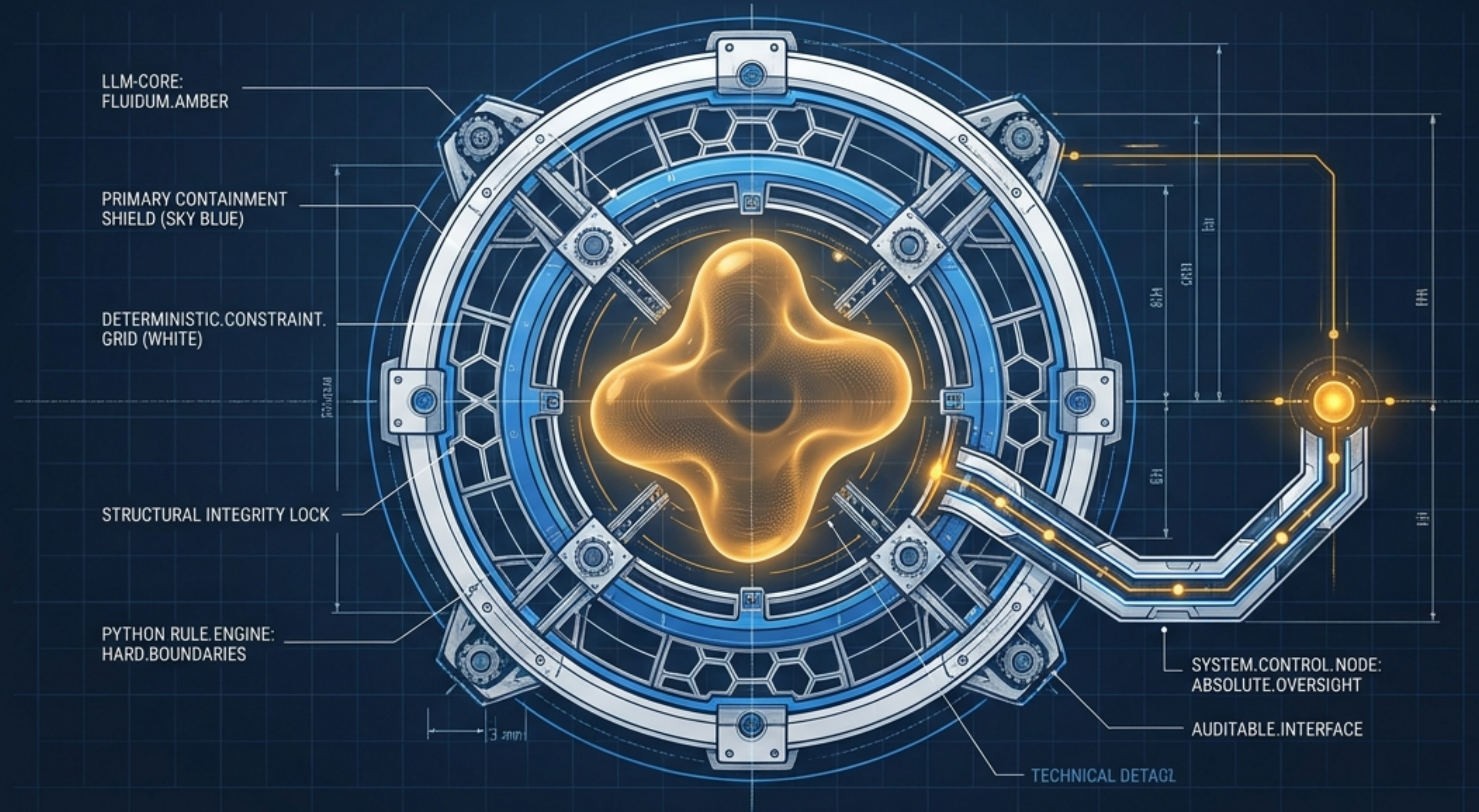


AUGUR: Die Architektur eines Senior-SEM-Agenten

Von unberechenbarem AI-Hype zu auditierbarer operativer Exzellenz



Das Problem: "Raw AI" agiert wie ein Junior-Marketer

Warum rohe LLMs an komplexen Senior-SEM-Aufgaben scheitern.

Erwartung



Proaktive Budget-Optimierung.

Realität



⚠ **Risiko-Aversion:** F1-Score = 0.0 für strategische PAUSE/BOOST Aktionen ohne harte Regeln (LLMs unter-committen systematisch).

⚠ **Kausale Halluzinationen:** Erfindet fiktive Cross-Cluster-Zusammenhänge (Attribution-Confound-Proof failed).

⚠ **Fehlende Constraints:** Keine inhärente Einhaltung statistischer Signifikanzen oder Budget-Schwellen.

Das Architektur-Paradigma: "Split-Brain" Reasoning

Exzellenz entsteht nicht durch mehr KI-Freiheit, sondern durch einen strikten deterministischen Käfig. Das Modell darf niemals das Regelwerk überschreiben.

Schicht 1: Deterministisch



Der Master:
Diktator der Action.

Properties:

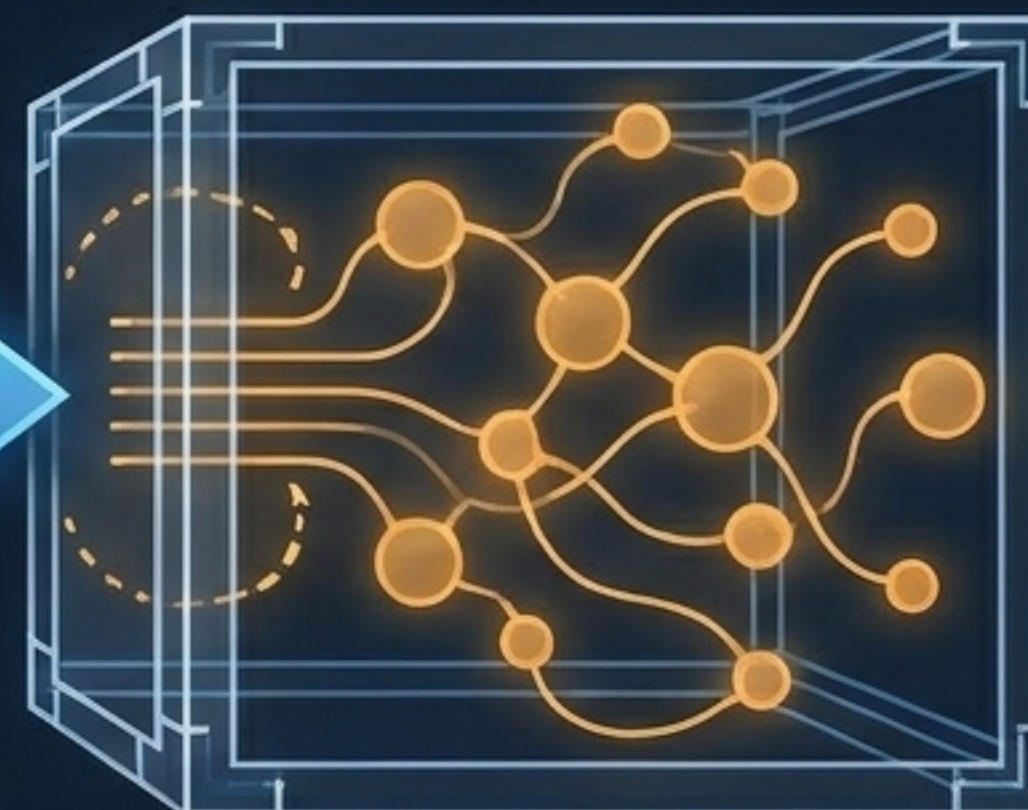
- ✓ Hard Constraints
- ✓ Python-Rules
- ✓ Auditierbar
- ✓ Reproduzierbar

Action erzwingt
Rationale

Properties:

- Formuliert Narrative
- Diagnostiziert Ursachen
- Ordnet Kontext ein

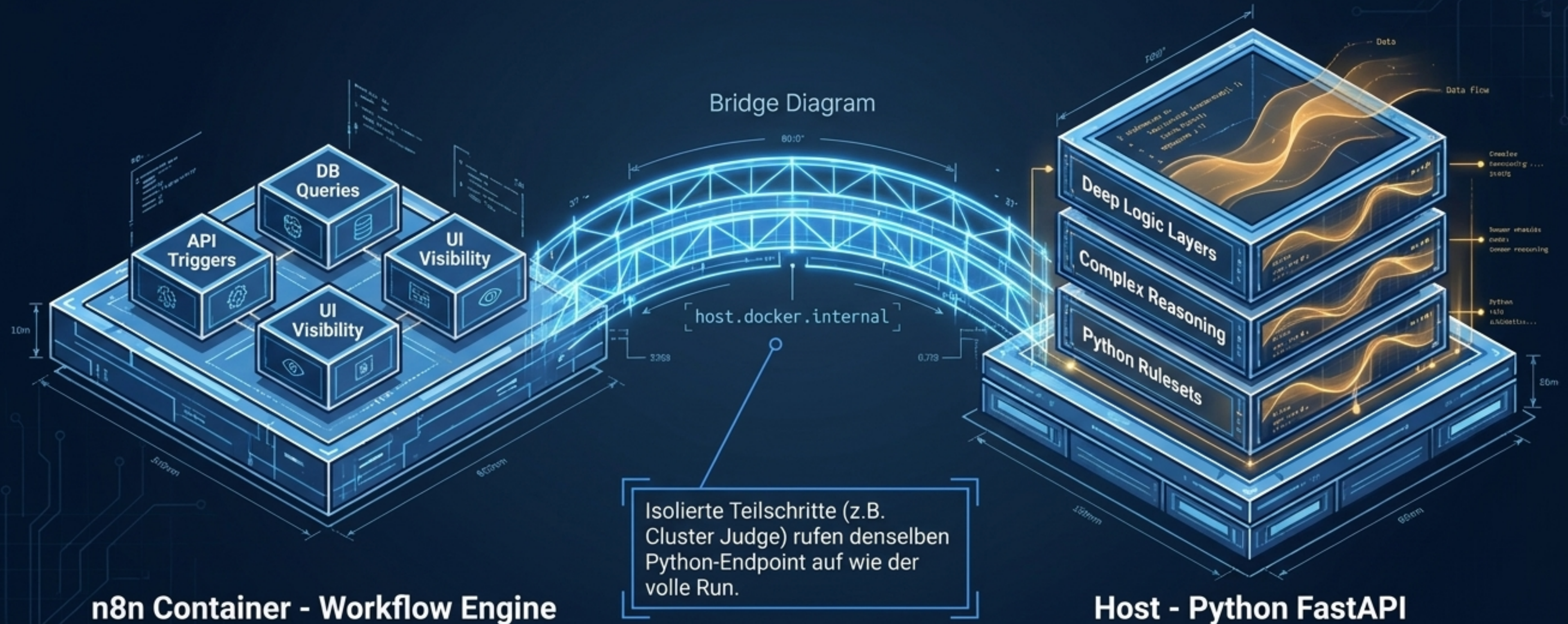
Schicht 2: LLM Analyst



Der Servant:
Synthese & Rationale.

Die Hybrid-Engine: Workflow-Orchestrierung trifft Python-Logik

Das "Variante B" Pattern: n8n fungiert als stabiler Backbone, FastAPI hostet die komplexe Agenten-Logik. Zero Logic Duplication.



Das "Soft-Fail" Designprinzip

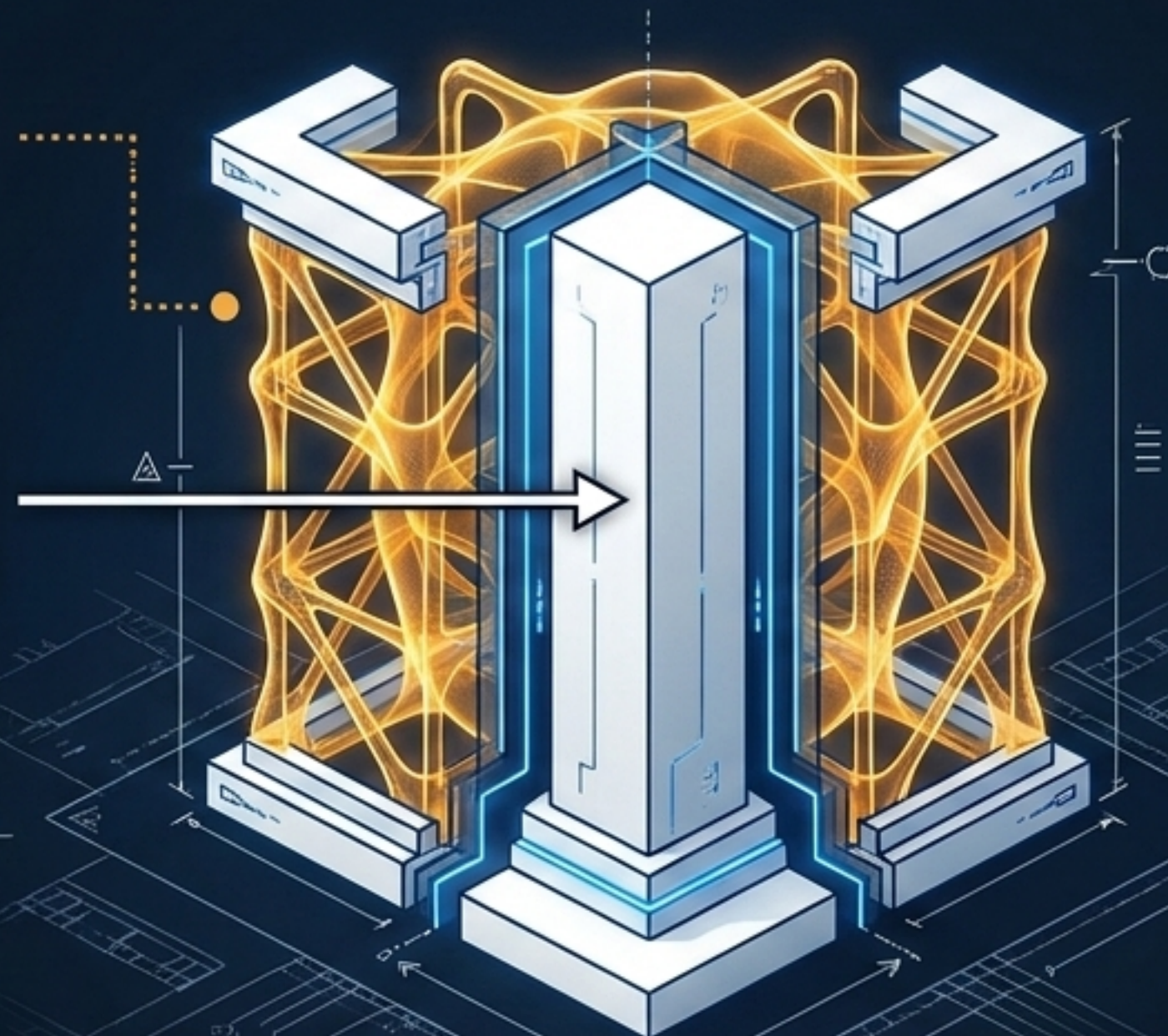
LLM-Instabilität wird als architektonische Konstante akzeptiert.
Die Basis-Wahrheit bleibt immer unangetastet.

LLM Cluster Judge

Nachgelagerte Soft-Fail-Schicht.
Darf nur hoch-konfidente Einzelzuordnungen korrigieren.

Deterministische Anker-Zuordnung

Unzerstörbares Fundament

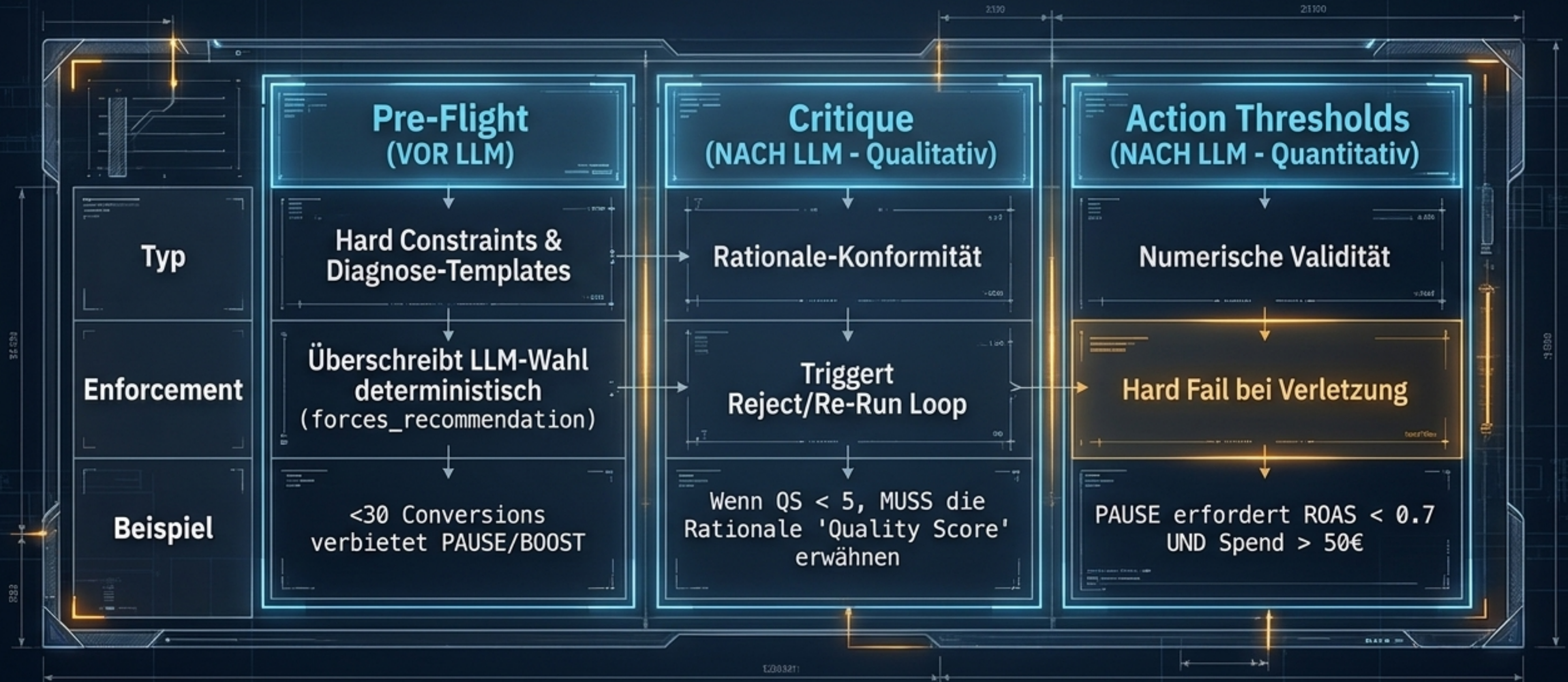


Fällt die KI aus (Timeout, Halluzination), läuft die Pipeline mit mathematischer Determinismus-Garantie weiter.

Kein Single-Point-of-Failure.

Das 3-Layer Defense System

Wie AUGUR durch sequenzielle Schichten schlechte KI-Entscheidungen systemisch unmöglich macht.



Granularitäts-Auflösung: Vom Rauschen zum Signal

401 Keywords erzeugen über 600 Regel-Matches. Wie verarbeitet das ein LLM? Gar nicht. Die Architektur aggregiert vorab.



Der Ehrlichkeits-Indikator

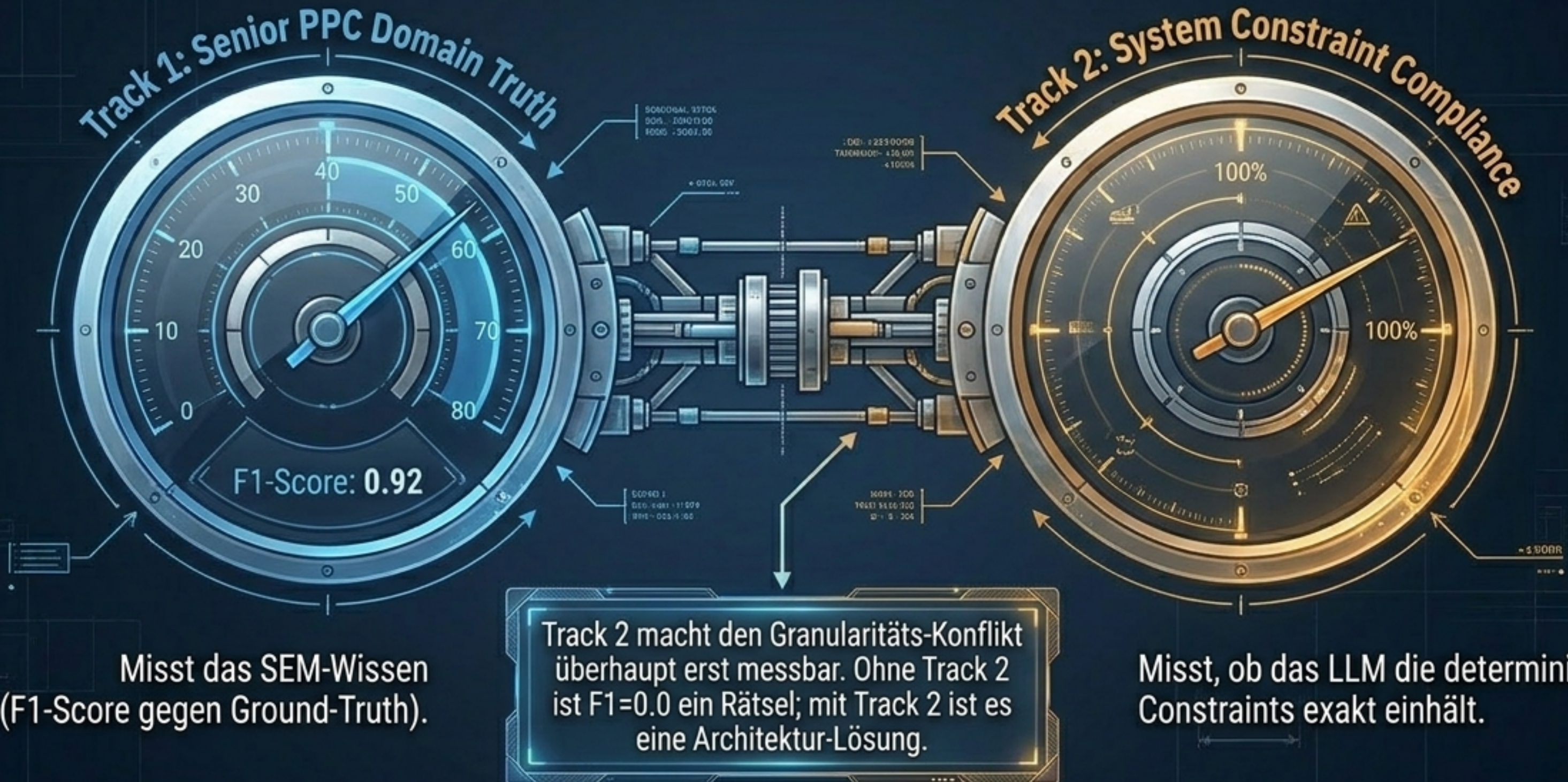
Ein radikal transparentes Audit: Wer trifft hier eigentlich die Entscheidungen?



F1-Score stieg durch diese Architektur von 0.125 auf >0.80. Der LLM ist der Schreiber, das System ist der Denker.

Dual-Track Evaluation Strategy

Ein einziger F1-Score verschleiert die Systemtreue. AUGUR trennt Domänen-Wissen von System-Compliance.



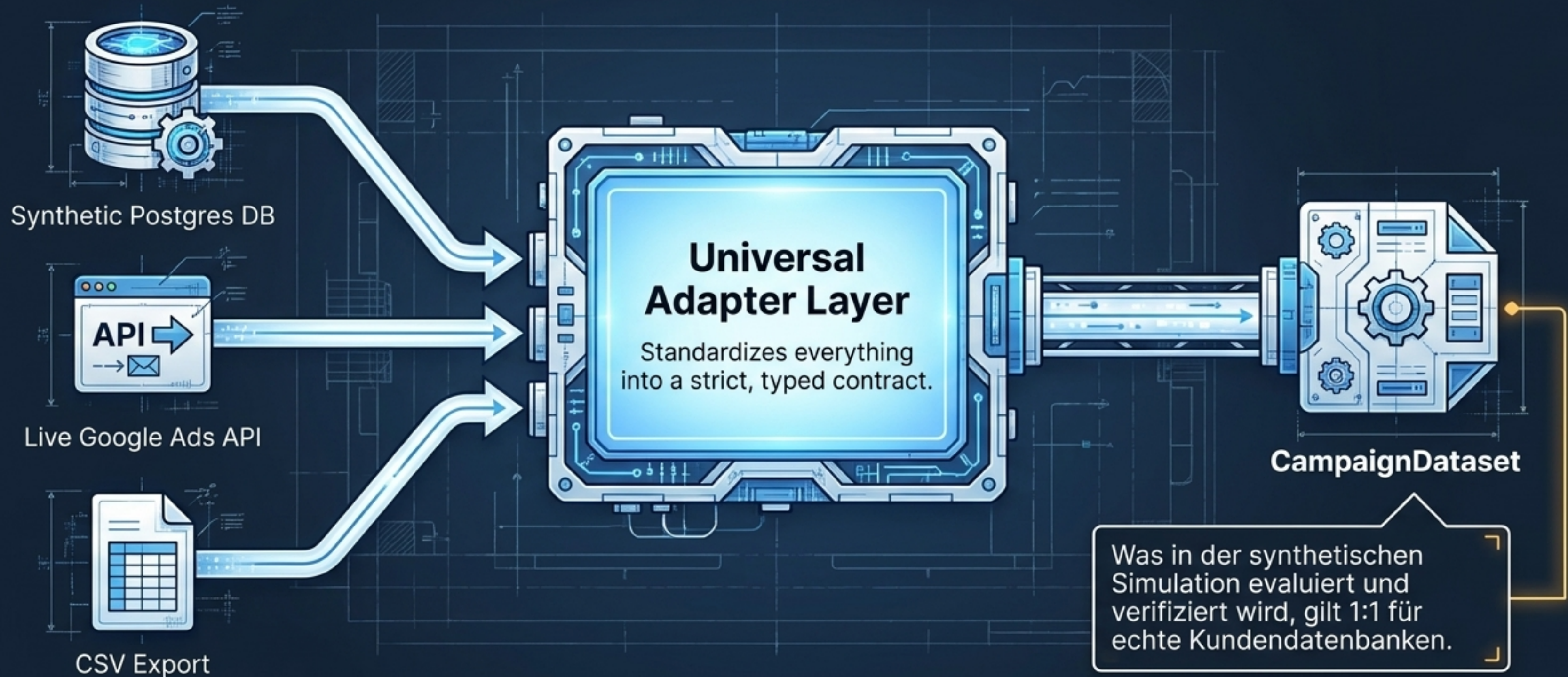
Asymmetrische Logik: Keyword vs. Cluster

Echte Seniorität bedeutet zu wissen, wann man streng rechnet und wann man strategisch abwägt.



Enterprise-Readiness: Der Adapter Layer

Die Core-Engine ist datenquellen-agnostisch. Kein Refactoring bei neuen Kunden.

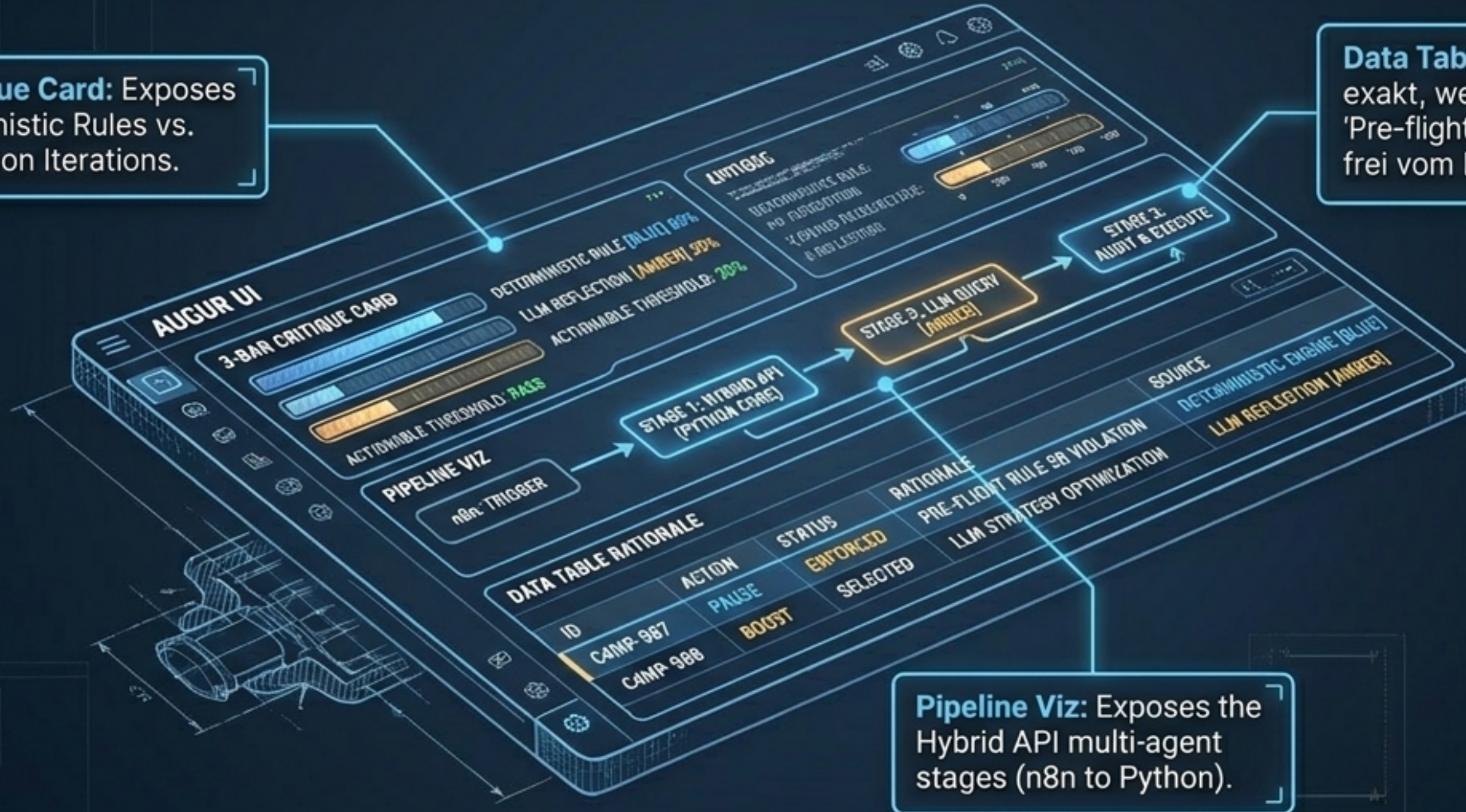


Das UI als sichtbare Architektur

Das AUGUR-Frontend ist kein Kosmetik-Layer. Es ist die Kontrolloberfläche für Stakeholder, um das 3-Layer-Defense-System live zu auditieren.

3-Bar Critique Card: Exposes the Deterministic Rules vs. LLM Reflection Iterations.

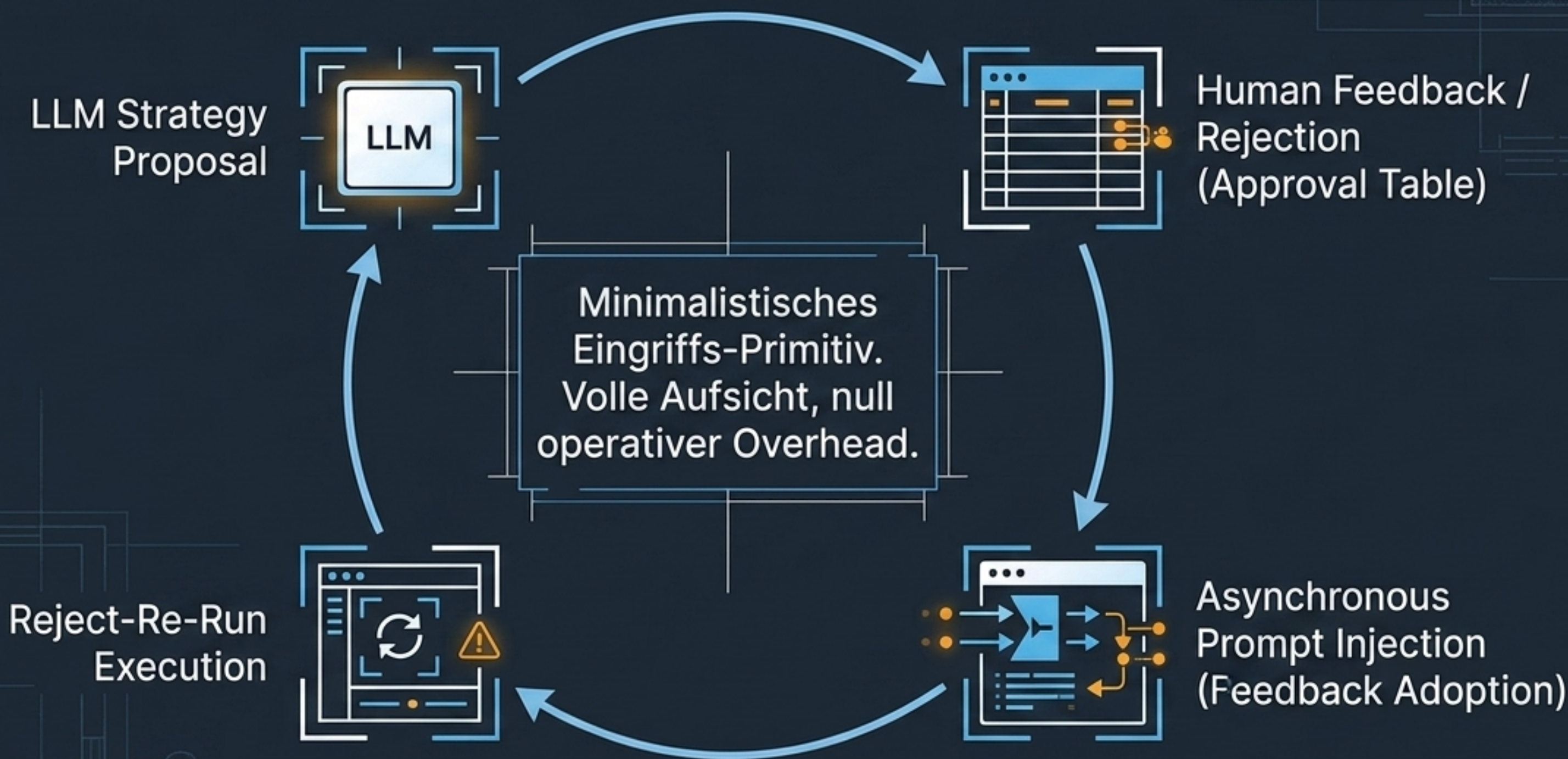
Data Table Rationale: Zeigt exakt, welche Action durch 'Pre-flight' erzwungen und welche frei vom LLM gewählt wurde.



Pipeline Viz: Exposes the Hybrid API multi-agent stages (n8n to Python).

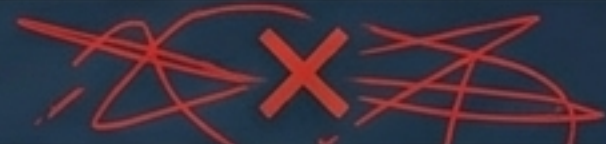
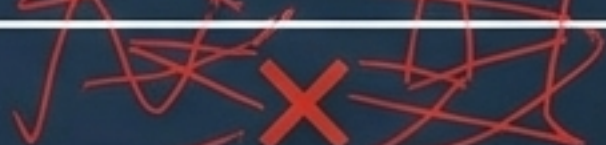
Control at the Edge: Human-in-the-Loop

Purer, asynchroner Operator-Eingriff ohne über-engineerte Workflow-Engines.



Der "Seniority Filter": Synthese

Was AUGUR grundlegend von einem generischen "AI Wrapper" unterscheidet.

	AI Wrapper	AUGUR Architecture
Deterministische Hard Constraints		
Quantitative Action Thresholds		
Erzwungene Diagnose-Schritte		
Dual-Track Evaluation		
Rationale Audit-Pflicht		

AUGUR übersetzt die Unberechenbarkeit von Sprachmodellen in die Verlässlichkeit einer Enterprise-Software.

Keine AI-Magie. Operative Exzellenz.

AUGUR transformiert SEM-Agentik in ein **verteidigbares**,
auditsicheres System für das Enterprise-Level.

