



Sichtbarkeit in OT-Netzwerken und Methoden der passiven Datensammlung

„You can't secure what you don't see" ► besonders in OT.



Ausgangslage: Blindflug im OT-Netz

- ▶ **Keine Transparenz**

Kommunikationsbeziehungen in der OT sind meist unsichtbar

- ▶ **Proprietäre OT-Protokolle**

Modbus, Profinet, DNP3 und Legacy Systeme

- ▶ **Verfügbarkeit vor Sicherheit**

Strikte Uptime-Vorgaben verhindern aktive Scans

- ▶ **Zielkonflikt OT vs. IT**

IT fordert Sicherheit, OT blockiert Eingriffe



Warum klassische IT Methoden in der OT scheitern

Das Grundproblem

IT-Security Methoden sind für OT-Umgebungen nicht gemacht, Sie gefährden schlicht das, was geschützt werden soll: **den stabilen Betrieb.**

- ☒ **Aggressive IT-Scans im OT-Netz**
Gefährden PLCs und SCADA Systeme
- ☒ **Software-Agents**
Auf OT-Systeme meist nicht installierbar
- ☒ **Inline - IDS/IPS**
Verursachen Probleme in OT-Netzen



Der **Emitec** Ansatz: Nur zuhören - Nicht sprechen

► **Passive** Zugangsschicht

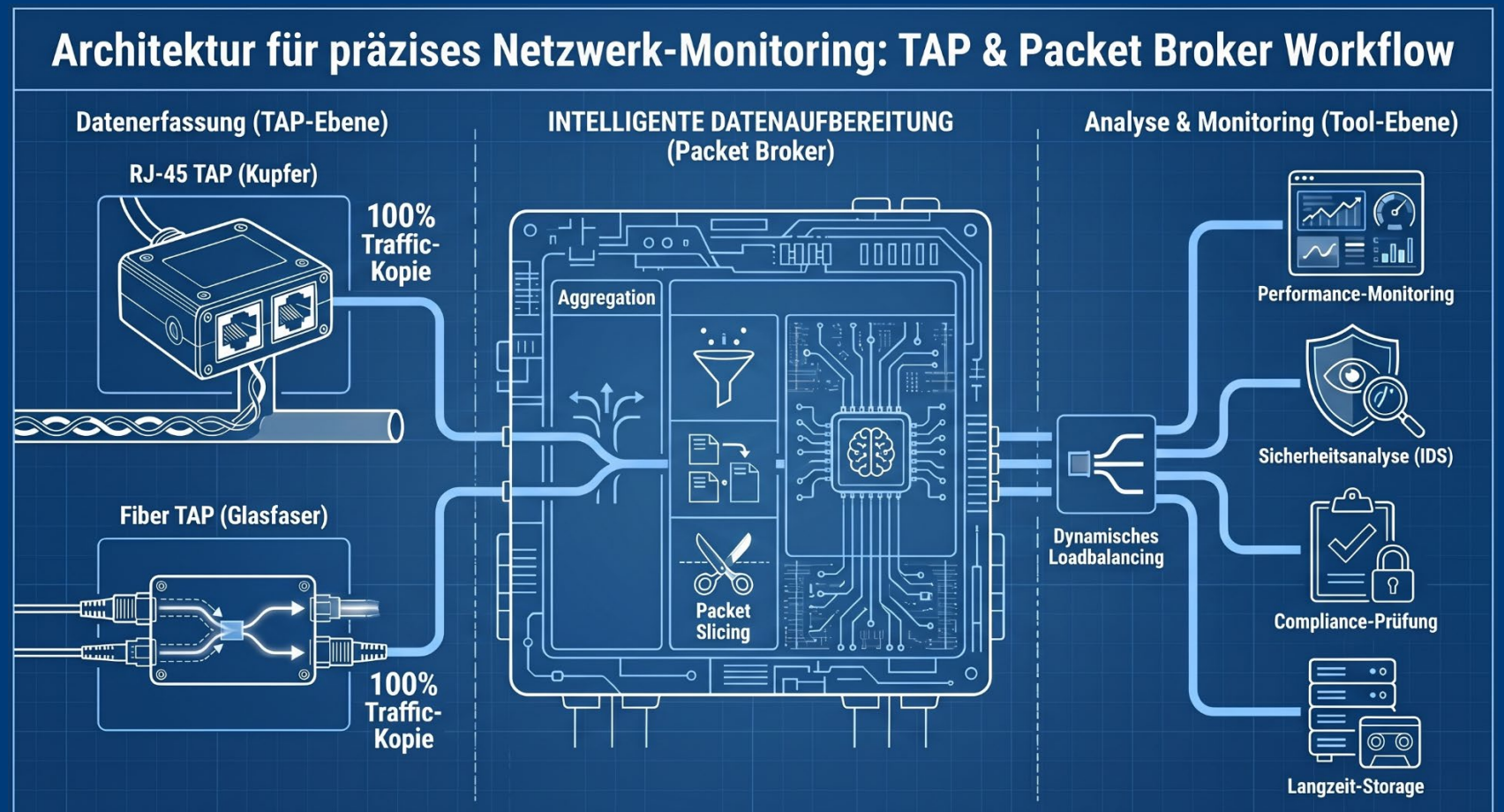
TAPs spiegeln Traffic 1:1

► **Traffic Aufbereitung**

NPB filtert und aggregiert Traffic

► **Tool & Probe Integration**

Probes und Tools erhalten gezielte, relevante Daten



Die **Basis:**

Effiziente Analyse und Kostenkontrolle

\$\$\$

Analyse Tool

Die teuerste Ebene

\$\$

Packet Broker

Der Schlüssel zur Kostenkontrolle

\$

Taps

Geringe einmalige Kosten

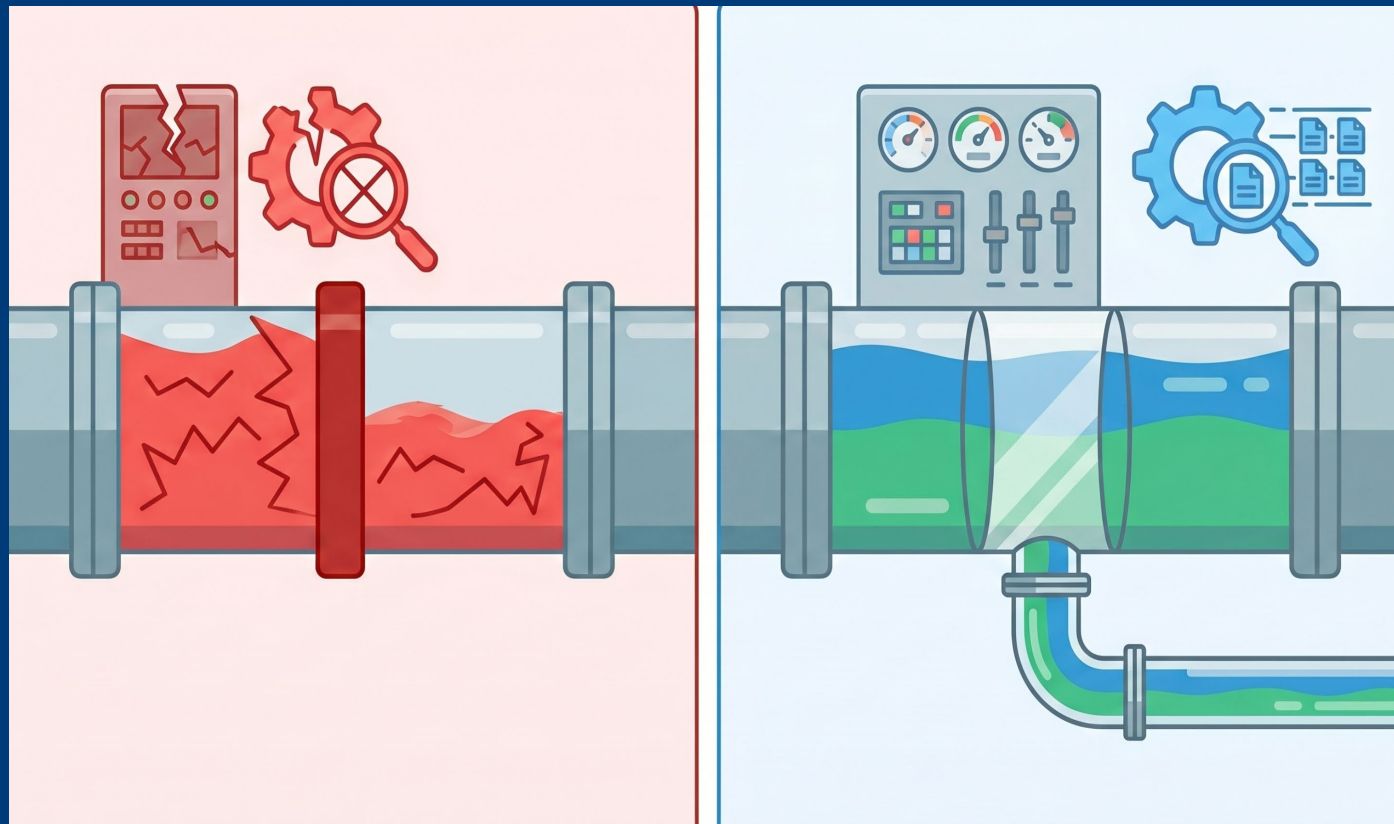
OT-Netzwerk

Bestehende Anlage




OT-Visibility ohne Unterbrechung

Vor der Inbetriebnahme

Nach der Inbetriebnahme



Ergebnis nach Inbetriebnahme

-  **Sichtbarkeit**
Alle OT-Assets bekannt.
-  **Transparenz**
Kommunikation klar nachvollziehbar
-  **Sicherheit**
Risiken erkannt, Betrieb unbeeinflusst



Takeaway



01

Sichtbarkeit ist die Basis

Ohne vollständige Transparenz
keine wirksame OT Security

02

Passiv heisst nicht eingeschränkt

Maximale Datentiefe – null Risiko
für den laufenden Betrieb

03

Die Basis wirtschaftlicher OT-Visibility

Taps und Network Packet Broker sind nicht optional – Sie sind die Lösung.
Ohne Sie keine saubere und skalierbare Analyse.

„OT Security beginnt dort, wo man sieht – ohne einzugreifen“

Besten Dank für eure Aufmerksamkeit