

Fig 1.

Fig. 1 — Pipeline-centric architecture for failure-intelligence
A request/run flows through policy → model → ingestion → event bus → classification → knowledge base → patterns → health, while the dashboard triggers and visualizes.

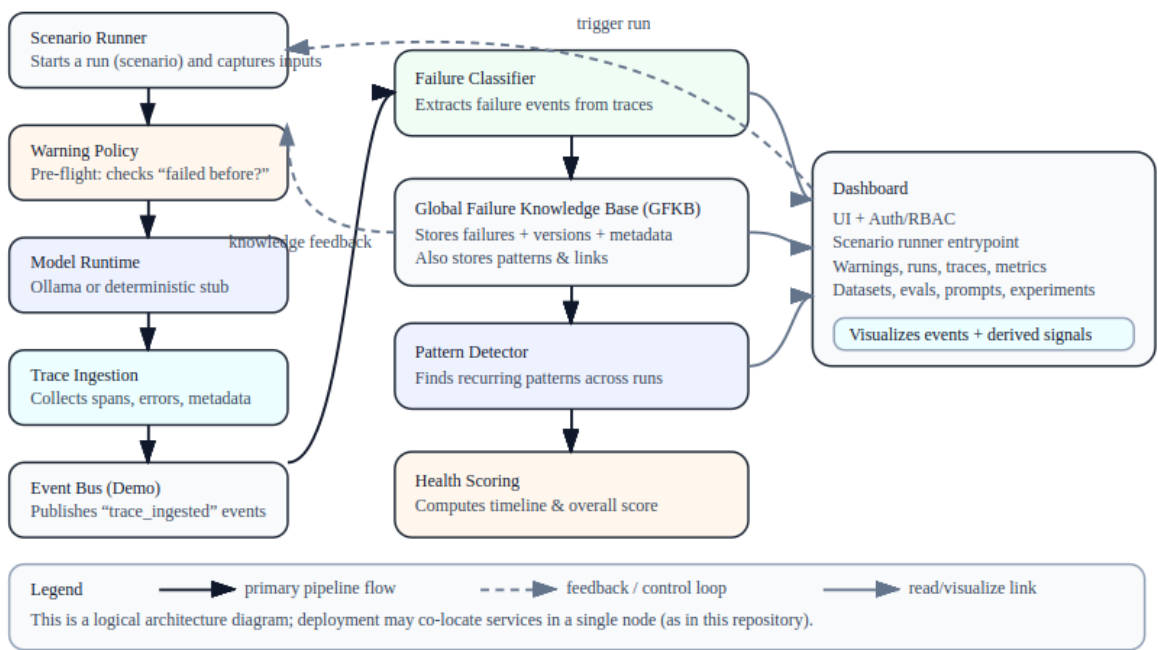


Fig 2.

Fig. 2 — Example data model for failure entities and pattern entities
Illustrative schema: failures are first-class records; patterns aggregate recurrent failures and link back to evidence runs/traces.

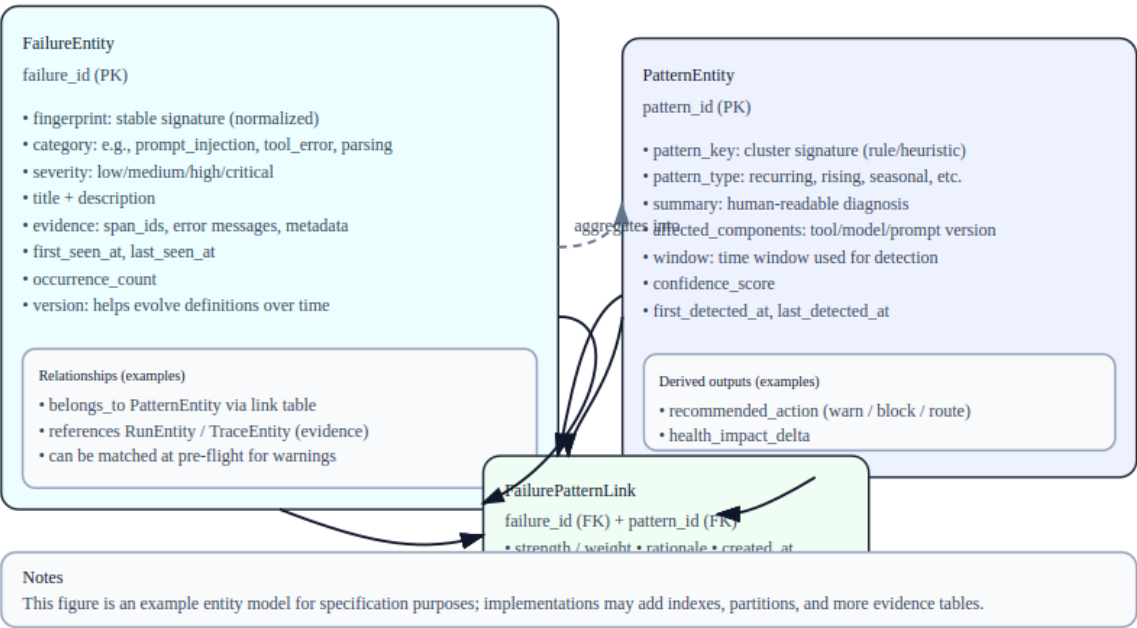
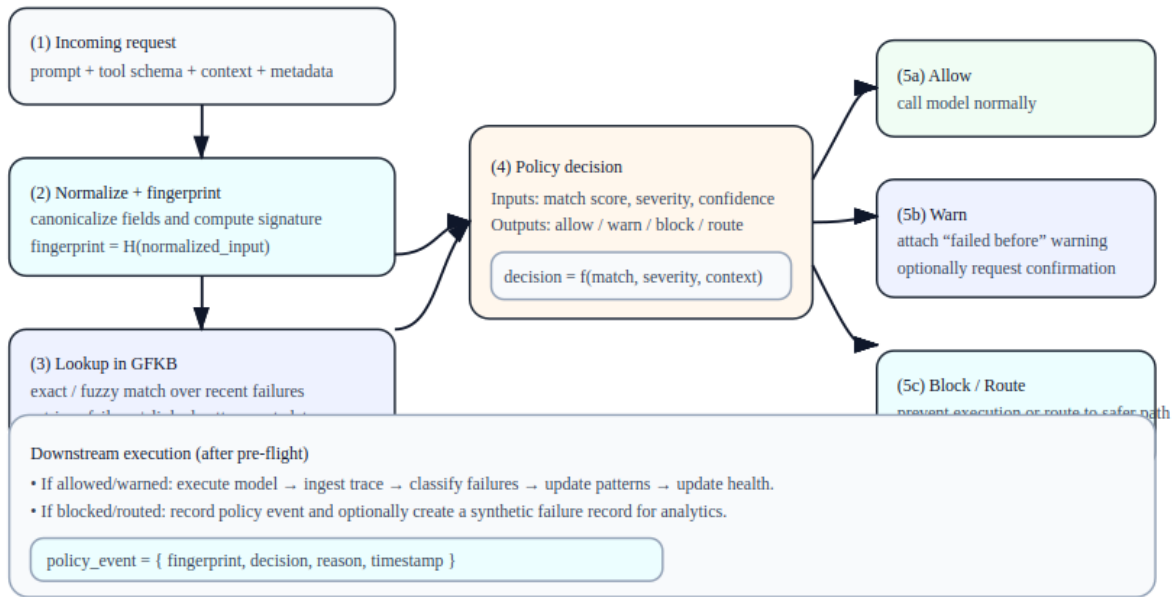


Fig 3.

Fig. 3 — Pre-flight matching and policy decision flow

Before calling the model, the system fingerprints the request, matches against failure memory, and applies a warning/block/routing policy.



Note: Matching may be exact (hash/fingerprint) or approximate (rule-based similarity / embeddings) depending on configuration.