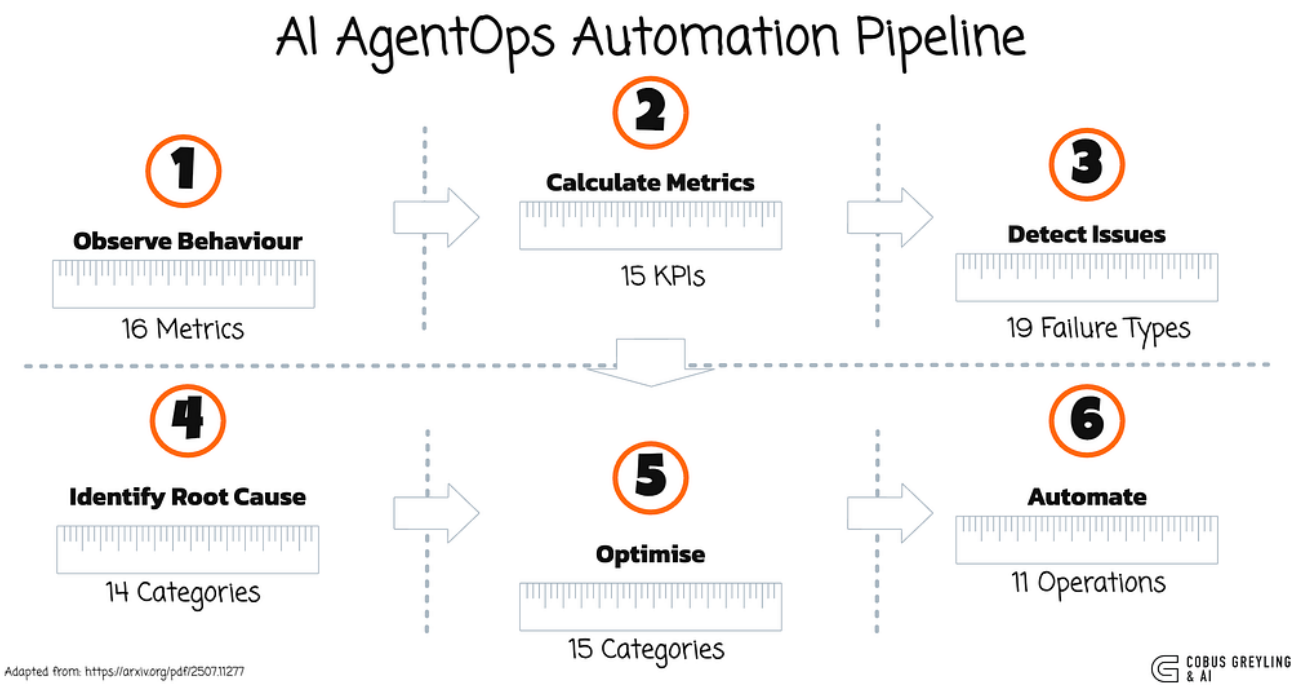
AI AgentOps

In a recent IBM study, researchers explore AI AgentOps, focusing on strategies to tame Generative AI without eliminating its agency — after all, agency inherently introduces uncertainty…

Cobus Greyling • 3 min read • 2025-08-18

https://cobusgreyling.medium.com/ai-agentops-0e06cfa12b97



In a recent IBM study, researchers explore AI AgentOps, focusing on strategies to tame Generative AI without eliminating its agency — after all, agency inherently introduces uncertainty…

For obvious reasons, an enterprise wants to control their AI Agents and have rigour in Operations…while also while not negating uncertainty…

> Uncertainty is intrinsic to intelligence

Reasoning & Ambiguity

> Just as we accept ambiguity in human reasoning, we must also recognise it in intelligent software systems.

But recognition does not imply surrender…

While agentic systems will inevitably exhibit behavioural uncertainty, the goal is to tame it — minimising the frequency and severity of undesirable or strongly suboptimal outcomes.

Promising directions for taming uncertainty through automation include:

Standardisation

The taxonomy lays the groundwork for **AgentOps**

• instrumentation,

• evaluation, and

• automation.

Graph-Based Analytics

Agentic systems generate structured, graph-like data with semantic depth.

New approaches should encode and use this data for detecting issues and analysing root causes.

Self-healing & Adaptive Execution

Automated systems need mechanisms to handle problems in real time, such as rerouting tasks, tweaking LLM parameters or changing execution plans.

This minimises suboptimal behaviour without constant human input.

Workflow enhancements include better task decomposition, step reordering for efficiency, parallelisation, and result reuse.

For invocations, systems cut redundant calls, choose optimal tools, apply throttling, and use intelligent retries to improve stability.

To boost resilience, systems add fallback strategies, monitor behavioural drift, enable error recovery, and implement guardrails.

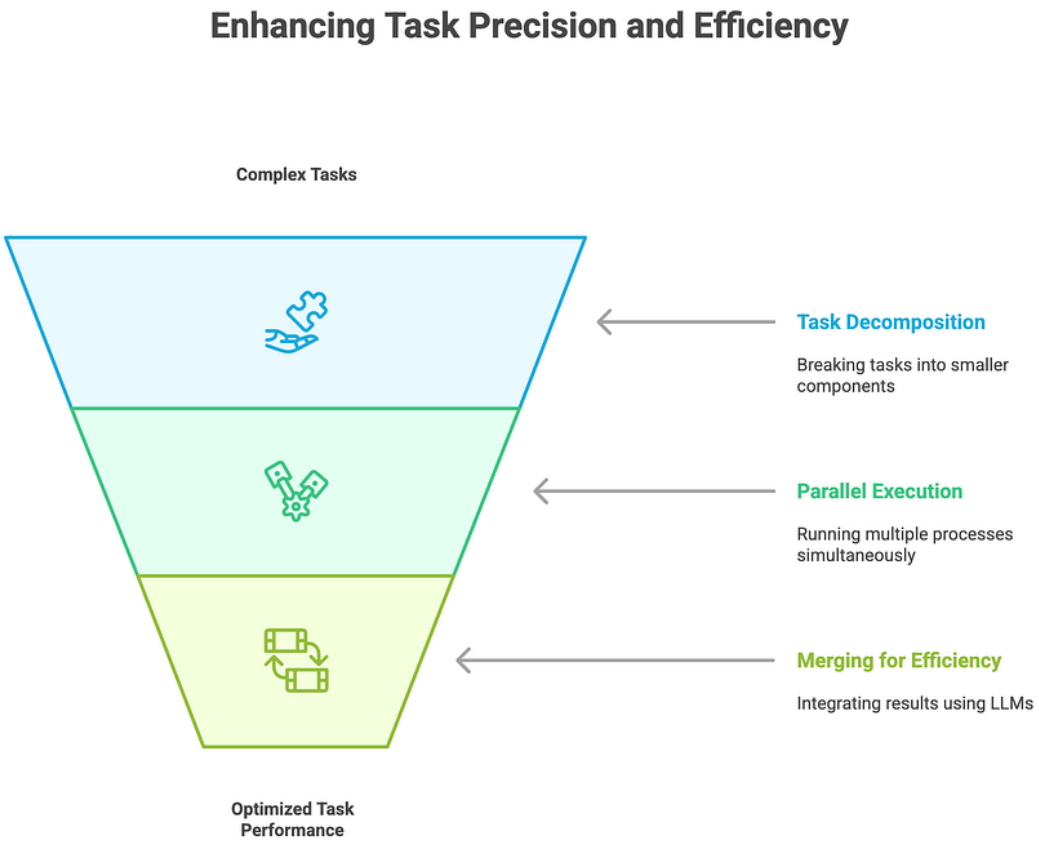
Optimisation Patterns

I found the identification of key optimisation patterns interesting…

Task decomposition for precision

Parallel execution to reduce latency

Merging for efficiency, often using large language models as evaluators.



AI Agent Monitoring Framework

Monitoring covers **79 points** across all pipeline stages for full visibility into agent operations from data ingestion to outputs. It detects anomalies early and checks the agent's lifecycle.

Automation efficiency allow**s 14% of operations to be fully automated** reducing manual intervention and speeding response times.

Critical failures show 24% of issues stem from LLM problems, like instruction, violations, hallucination and prompt inaccuracies.

> This requires better model training and prompt engineering to reduce risks.

Optimisation potential has 19%, focused on resilience and reliability improvements using redundancy and error-handling for consistent performance.

Operations use 5 metric categories:

1. Development (build quality)

2. Evaluation (accuracy)

3. Maintenance (stability)

4. Business (goals) and User

5. Perspective (satisfaction).

Security and compliance account for 26% of issues involving violations data exposure and breaches. Address them with encryption **audits** and **compliant designs** to protect data.

🔍 Monitoring Scope

79

Total monitoring points across all pipeline stages, ensuring comprehensive coverage of agent operations.

⚡ Automation Efficiency

14%

Of total operations can be fully automated, reducing manual intervention and improving response times.

🎯 Critical Failure Points

24%

Of issues stem from LLM-related problems (instruction violations, hallucination, prompt accuracy).

🔧 Optimization Potential

19%

Of optimizations focus on resilience and reliability improvements for better agent performance.

📊 Metric Categories

5

Core metric types: Development, Evaluation, Maintenance, Business, and User Perspective.

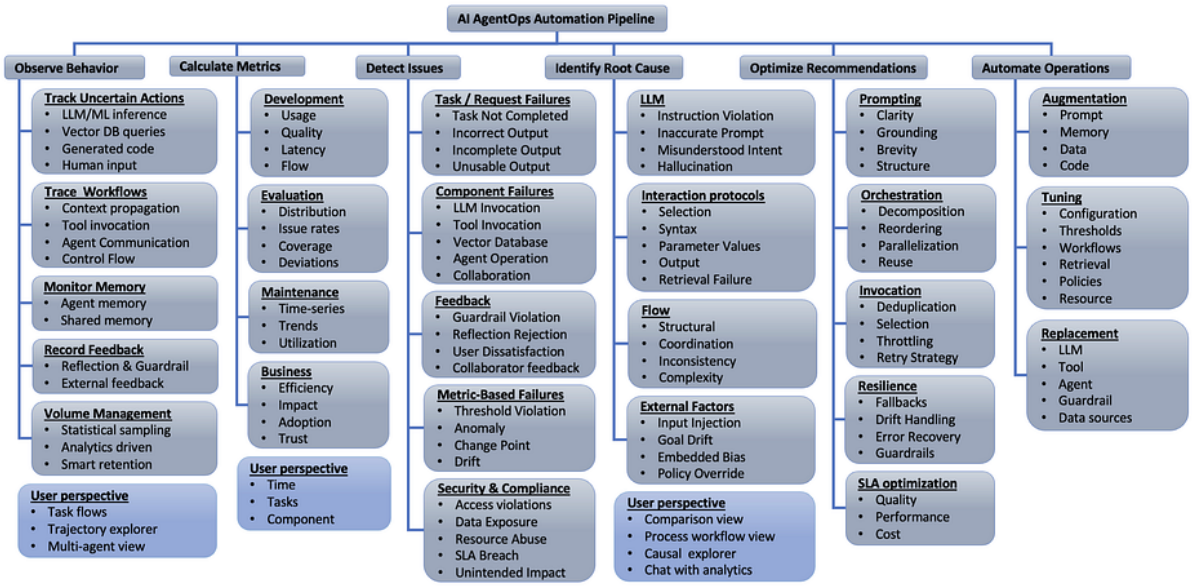
🛡️ Security & Compliance

26%

Of detected issues relate to security violations, data exposure, and compliance breaches.

Adapted from: https://arxiv.org/pdf/2507.11277

COBUS GREYLING & AI



Passive analytics for deriving insights on metrics like

• cost,

• latency and

• token usage

through task flow graphs.

Chief Evangelist *@ Kore.ai | I'm passionate about exploring the intersection of AI and language. Language Models, AI Agents, Agentic Apps, Dev Frameworks & Data-Driven Tools shaping tomorrow.*

Other mentions by Author

• arxiv.org | Taming Uncertainty via Automation: Observing, Analyzing, and Optimizing Agentic AI Systems

• www.cobusgreyling.com | COBUS GREYLING

• opentelemetry.io | AgentOps Automation Pipeline

• cobusgreyling.medium.com | Written by Cobus Greyling