GenOps: Govern AI for High-Velocity CI/CD

SPEAKER

Neeraj Kumar Singh Beshane

Conf42 DevOps 2026

Staff Security Infrastructure Engineer @ *Parafin*

Specializing in Security, DevSecOps infrastructure, CI/CD automation, and AI integration at scale. Passionate about building governance frameworks that enable safe, high-velocity software delivery in enterprise environments.

CONTEXT

The AI Paradox: Bridging Adoption to Impact

The Promise

88% Adoption

Engineering teams actively deploy AI

~55% Productivity Speed

Faster delivery without compromising safety standards

The Price

$12.9K Cost/Min

Average production outage expense

2,100+ Downtime Hours

Jira degradation in 2024

7.2% Stability Drop

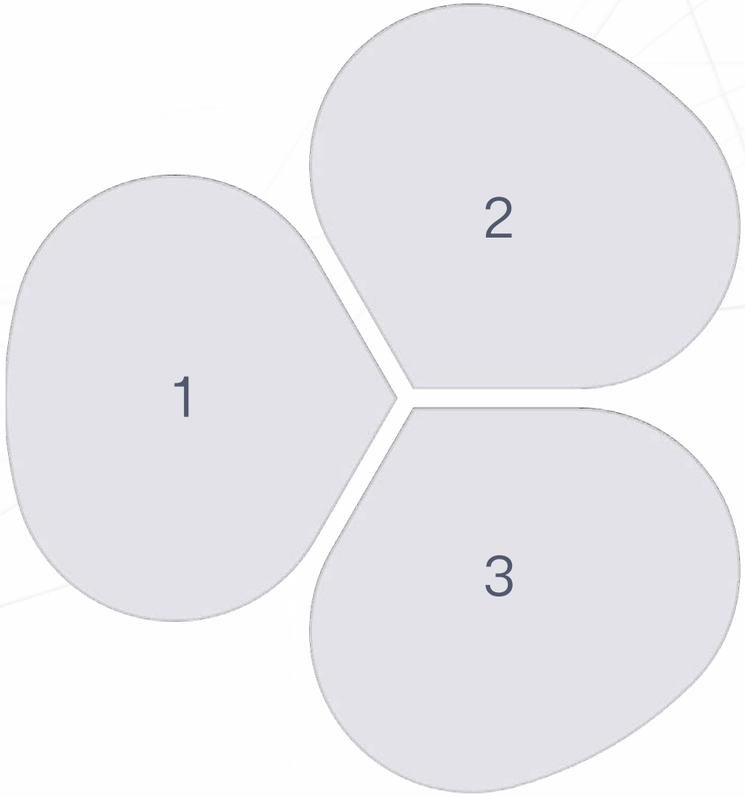
AI adoption may negatively impact software delivery performance

Source: *Microsoft Status History 2024, Google Cloud 2024, State of DevOps Report*

Unlocking AI's Potential: The Integration Dilemma

Taming AI's Unpredictability

Generative AI injects inherent unpredictability into mission-critical CI/CD pipelines, demanding robust strategies for consistency.



Preventing Systemic Disruptions

Operational instability can devastate entire delivery systems, jeopardizing multiple teams and critical services.

Reconciling Safety and Speed

Traditional approaches impose a false choice between rapid deployment and unwavering reliability. It's time for a new paradigm.

PARADIGM SHIFT

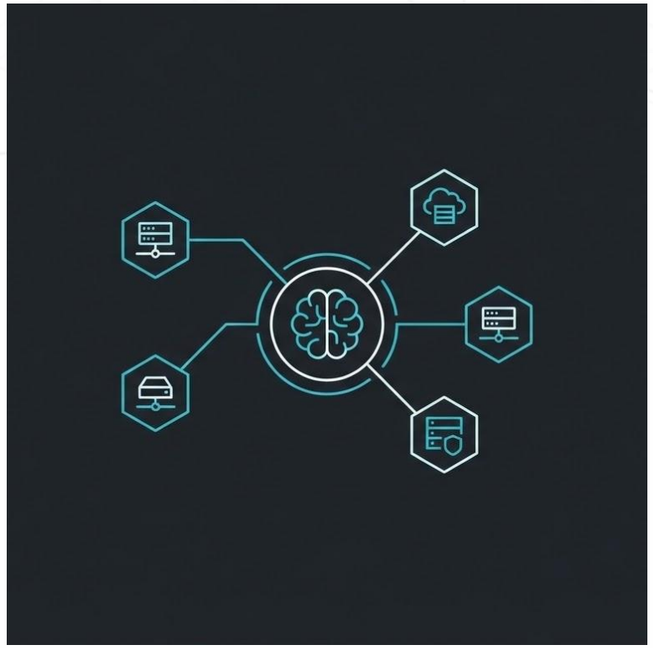
Unleashing GenAI: From Tool to Trusted Partner

Legacy AI: External & Unaccountable

AI traditionally serves as an external helper, disconnected from core pipeline execution and lacking direct accountability.

GenOps: Integrated & Governed AI

GenOps positions AI as a governed Pipeline Actor, bound by explicit SLOs, stringent safety, and enterprise governance frameworks.



Fortifying AI: The Four Pillars of Governance

Dynamic Contextualization

Leverages RAG for comprehensive build history and deployment metadata.

Strategic Probabilistic Guardrails

Implements robust guardrails with service-tier error budgets.

Adaptive Canary Deployments

Ensures automated kill switches and continuous SLO monitoring.

Continuous Runtime Assurance

Drives model registry alignment and immutable audit compliance.

Together, these pillars forge a closed-loop, safety-aware system, empowering AI to predictably and securely enhance DevOps workflows.

PILLAR 1

Fuel AI Decisions: Context-Aware Ingestion

Grounding AI with Real-Time Context

Integrate build history, deployment logs, and infrastructure metadata to anchor AI decisions in current operational realities.

1

Eliminate AI Blind Spots

Prevent hallucinations and flawed recommendations by empowering AI models with comprehensive system intelligence.

2

Continuously Evolve AI Knowledge

Dynamically refresh the knowledge base with every deployment, ensuring sustained accuracy and relevance for evolving environments.

3

PILLAR 2

Deploy with Confidence: Guardrailed AI Planning

Safeguard critical services. Our AI decisions operate within strict guardrails, ensuring generative actions never exceed acceptable risk tolerances.

Strategic Error Budgeting

Define clear error budgets for each service tier.

Quantify Risk: Blast Radius Scoring

Assess change impact through blast radius analysis.

Automate Decision Boundaries

Establish strict boundaries for AI-driven actions.

Set Escalation Thresholds

Define clear thresholds for high-risk changes.

PILLAR 3

Secure Faster Releases with Staged Canary Rollouts

Pilot Canary Deployment

Deploy to 1-5% of traffic; ensure intensive monitoring.

Expand Incrementally

Gradually scale rollout based on strict SLO adherence.

Automate Rollbacks

Enable kill switches to trigger on SLO drift detection.

PILLAR 4

Runtime Governance

Centralize Model Tracking

Track approved AI models, versions, and performance from a single source.

Generate Comprehensive Audit Trails

Log AI-driven decisions for compliance and deep analysis.

Enforce Real-time Policy

Validate AI agent behavior dynamically against defined policies.

RESULTS

Unwavering Safety: Precision Governance in Action

Fortifying Operational Integrity

55 %

Zero Safety Bypasses

100% Protocol Adherence

No Error Budget Breaches

100% Prevention Rate

Accelerated Cycle Times

Faster delivery without compromising safety standards.

Why Zero?

14.4% of deployments **blocked** by Canary gates, proactively preventing unstable releases.

Catastrophic failures averted BEFORE production, safeguarding millions and reputation.

> Governance embedded in architecture is more reliable than governance as policy overlay.

Github: @neerazz/genops-framework

GenOps: The Next Frontier in DevOps Safety

Static Analysis: Code at Rest

- Scans code quality, but only at rest.
- Lacks runtime or operational context.

Code Assistance: Speed over Safety

- Accelerates code writing.
- Doesn't enforce pipeline safety or governance.

Anomaly Detection: Reactive Response

- Identifies problems only after they occur.
- Limited prevention or root cause understanding.

GenOps: Proactive Intelligent Safety

- Drives generative decision-making within the delivery pipeline.
- Establishes a closed-loop, safety-aware DevOps system.

ARCHITECTURE

Achieve Continuous Delivery with Our Closed-Loop System

Monitor

Proactively track SLOs

Analyze

Derive context-driven insights

Learn

Continuously integrate feedback

Act

Execute with governed automation

KEY TAKEAWAYS

Driving Innovation: Our Path Ahead

1 Governance Accelerates Innovation

Rather than impede, smart governance instills confidence, empowering teams for rapid, secure iteration.

2 AI: A Pivotal Pipeline Actor

Seamlessly integrate governed AI into CI/CD to unlock transformative improvements and operational excellence.

3 Embrace Closed-Loop Systems

The future of DevOps lies in self-correcting systems that learn, adapt, and operate within explicit safety boundaries.

Thank You!

Questions?

Neeraj Kumar Singh Beshane

Staff Security Infrastructure Engineer, **Parafin**