AUTHOR

Alexandru Muresan, a.muresan@student.tudelft.nl

SUPERVISORS

Eileen Kapel, Prof. Diomidis Spinellis

What Secondary Issues Contribute to Operational Problems?

An Investigation Based on Public Postmortems

AFFILIATIONS

EEMCS, Delft University of Technology

01. Introduction

- Operational incidents can disrupt services, cause financial loss, and harm reputation.
- Most research focuses on primary faults (**bugs, misconfigurations**).
- However, secondary issues, such as **poor communication** or **bad monitoring**, are less studied but often worsen incidents.
- This project uses public postmortems (**VOID & GitHub**) to uncover patterns in secondary issues.
- It builds on AIOps (AI in IT Operations) to scale incident analysis using large language models.

02. Project Purpose

- Identify systemic weaknesses that amplify operational failures.
- Analyze real-world incidents for patterns in:
- 🧠 Human factors (communication, documentation)
- 🔍 Monitoring issues
- ⚙️ Automation gaps and rollback deficiencies

03. Research Questions

- **RQ1:** What **secondary issues** are present in the data?
- **RQ2:** Are there patterns linking the most frequent secondary issues to specific **primary faults**?
- **RQ3:** Which secondary issues are often **found together**?

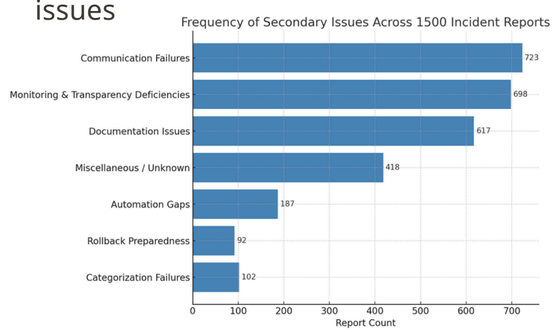
04. Methodology

- 🌐 1,500 public incident postmortems from GitHub and VOID
- 🐍 Python-based **web scraping**
- 🗂️ Classification of secondary issues (7 types)
- 🧠 Text preprocessing + **LLaMA 3 (70B & 8B)** for classification via groq
- 📄 Prompted LLMs identify secondary issues
- ✅ **Manual validation** on 100 random reports
- Outputs structured, normalized, and analyzed statistically

05. Results

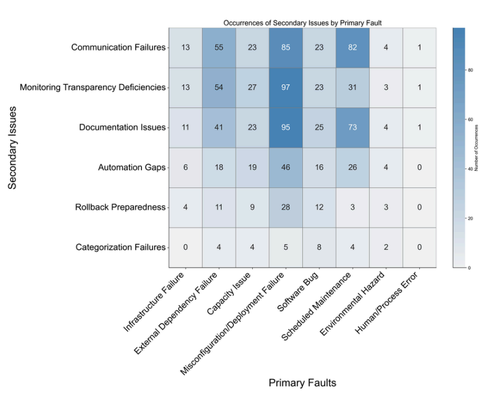
This project reveals patterns in secondary issues that impact incident outcomes across large-scale systems.

- 📈 Frequency analysis across **1,500 reports**
- 🔗 Patterns between **secondary issues and primary faults**
- 🧩**Co-occurence** between secondary issues

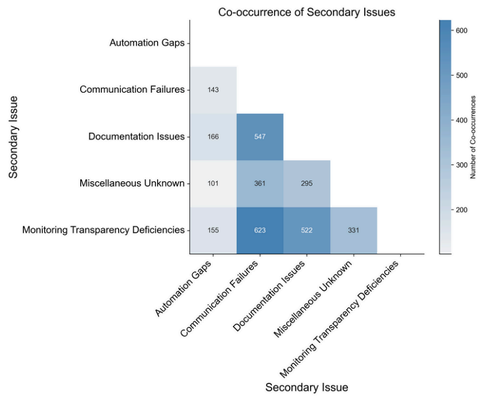


06. Analysis

Graphs generted using matplotlib to help with visualization



Heatmap containing the link between secondary issues and primary faults



Co-occurence heatmap showing which secondary issues tend to co-occur

07. Discussion + Future Work

Discussion:

- Most common issues: Communication, Monitoring, Documentation
- Frequent co-occurrence => systemic interdependence

Future directions:

- Expert-led annotations
- Private/internal postmortems
- More strict prompt/LLM tuning
- Larger, more diverse datasets

08. Conclusion

- Secondary issues amplify incident severity/duration
- Patterns emerge across 1,500 public reports
- **LLM pipeline** enables scalable, reproducible analysis
- Insights support **better response, resilience, training**
- Demonstrates value of analyzing postmortems at scale, beyond individual case studies
- Encourages shift from **fault-centered thinking to systemic awareness** in incident management
- Highlights the need for improved organizational practices alongside technical solutions