Architecting for Resilience: Strategies for Fault-Tolerant systems

Maria Rogova

Type of failures

- Hardware
- Network
- Human error
- Environmental
- Security breaches

Requirements?

- Monitoring
  - Automation detection
- Testing: testing environment, stress testing, tools testing
- Tools & runbooks
  - Automate everything
- Chaos engineering
- Incremental rollout

System Design

Architecture

- Architecture: modular, distributed, scalable
- Dependency Management & Single point of failure
  - Internal & external dependencies
- Graceful degradation & Failover
  - Adaptive UI
- Diversity

Redundancy

- Hardware (RAID, hot standby)
- Software (N-Version programming, process replication)
- Network (multiple network paths)
- Data (data mirroring, backup)
- Geographical (multi-data center deployment)

- Google: on 13th August 2015 4 successful lighting strikes
- Twitter and Instagram July 14, 2022 both went down because of unrelated reasons
- 12th of January 2024, a lot of descriptions of items in Amazon been replaced with "I apologies but I can't fulfil this request."