

# Robust AI System

## System-Level Faults

- ▶ Bit Flips
- ▶ Component Wear-out
- ▶ Memory Errors
- ▶ Power Failures
- ▶ Temperature Extremes

## Input-Level Attacks

- ▶ Adversarial Attacks
- ▶ Data Poisoning
- ▶ Prompt Injection
- ▶ Input Manipulation

## Environmental Shifts

- ▶ Data Drift
- ▶ Concept Drift
- ▶ Domain Shift
- ▶ Distribution Changes
- ▶ Context Evolution