# 17-423/723: Designing Large-scale Software Systems

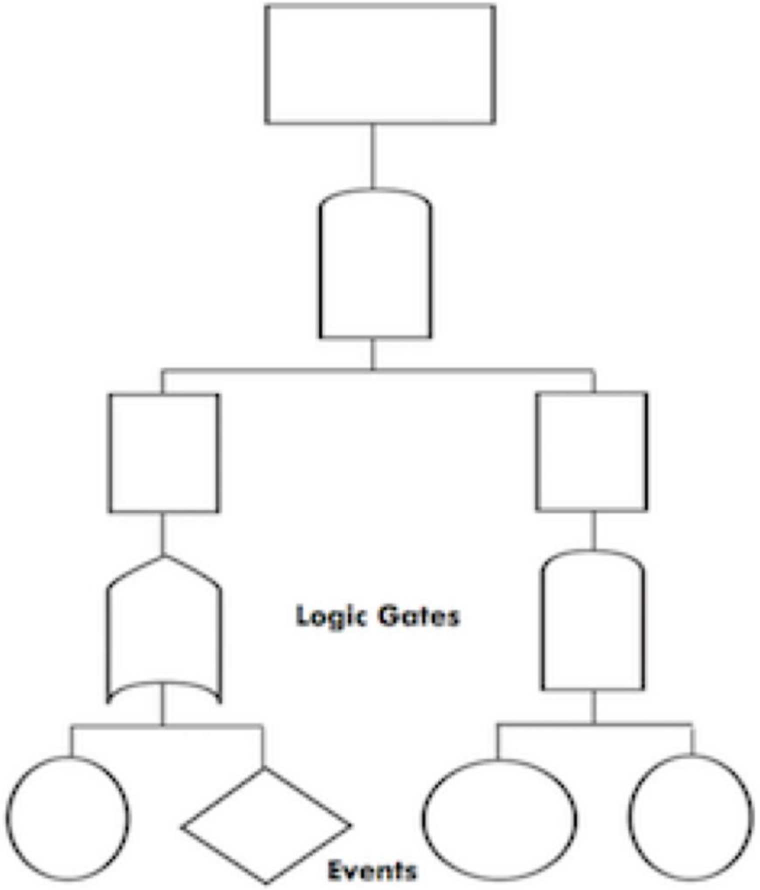
## Recitation

Design for Robustness

Mar 28, 2025

# Recall: Fault Tree Analysis (FTA)

- **Fault tree:** Specify relationships between a system failure (i.e., requirement violation) and its potential causes
  - Basic events correspond to a component failure or a violation of an environmental assumption
- **Minimal cut set**: A minimal set of basic events whose simultaneous occurrence is sufficient to guarantee that the TOP event occurs



# Recall: IntelliGuard from HW1

# Activity #1: FTA for IntelliGuard

- Recall **IntelliGuard** from HW1
- Break into groups; pick one person’s design from HW1
- Develop a fault tree for the following event: “The intrusion detection system fails to notify the homeowner in time when a stranger appears around the house.”
- Identify the minimum cut sets in your fault tree

# Recall: Design Patterns for Robustness

- Guardrails
  - Preconditions, interlocks, doer-checker
- Redundancy
  - Hot standby, voting, sensor fusion
- Separation
  - Circuit breaker, bulkhead pattern
- Graceful degradation
- Human in the loop

# Activity #2: Redesign for Robustness

- Redesign the system to improve its robustness against possible system failures identified using the fault tree
    - Pick a minimum cutset from the tree
    - Apply one or more design patterns to address the basic events in the cutset
        - Remove a basic event, or
        - Expand the cutset by requiring additional basic events to occur
    - Modify the fault tree to reflect the new design of the system