# People Helping Systems:
# Workarounds and System Dependability

RoSES

Christopher Martin
Prof. Philip Koopman

## Goal:

What can we do to better evaluate and quantify mission level dependability?

## Observation:

Humans can sometimes help systems work around partial failures.

## Approach:

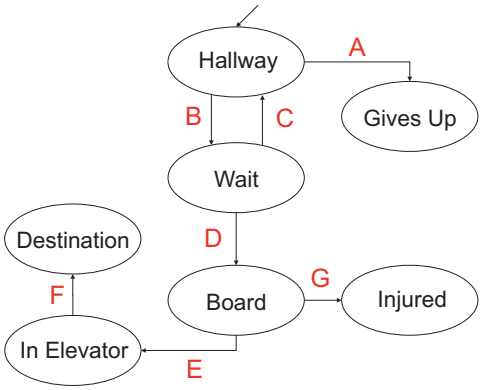
Mission graphs can be used to identify and suggest workarounds to mission-level dependability bottlenecks.

## Exploration:

Represent an example system via a mission graph and investigate the effects workarounds have on system dependability.

### Example System: An Elevator

- Here, we take an existing, complex simulation of an elevator and its users and represent it using a mission graph.
- Using this model, we can simulate the effects of proposed design changes that enable users to work around partial system failures.




Mission graph of example elevator system

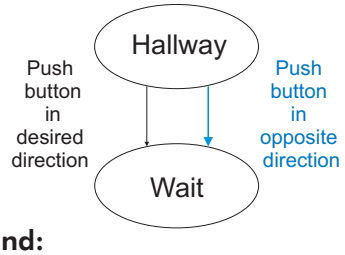
| Arc | Description |
|---|---|
| A | User times out (frustrated) |
| B | User presses call button |
| C | User times out (excessive wait) |
| D | Doors open / lanterns activate |
| E | Doors close on user |
| F | User boarding time elapses |
| G | Doors close, elevator travels to destination |

## Results of Incorporating Workarounds in the Example System:

### Hardware Redundancy

- Exploit heterogeneous redundancy to provide alternate paths
- Move beyond brute force redundancy, traditional reliability measures

Proposed Workaround:

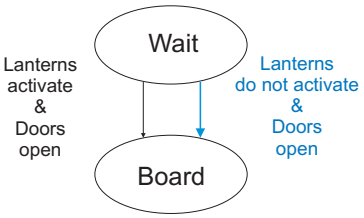



**Result of enabling workaround:**
Under moderate passenger loads, **average delivery time reduced up to 200%** when buttons were broken.

### User Interface

- Provides paths that correspond to user flexibility
- Shed performance in light of partial system failures

Proposed Workaround:

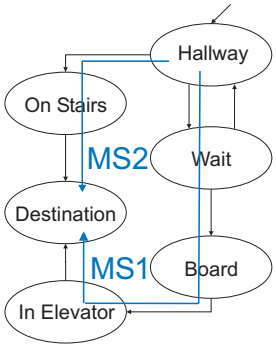



**Result of enabling workaround:**
Previously undeliverable passengers were **delivered with only a 1% performance penalty** compared to a fully functioning system.

### Global / Non-Technical

- Systems that are performing according to specifications can still be "broken" from a practical perspective.
- Alternate paths can provide a "safety valve" for overly stressed systems.

Proposed Workaround:

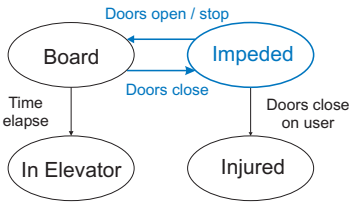



**Result of enabling workaround:**
Under heavy passenger loads, **delivery times reduced by 50%.**

### Recovery

- Change system to a useful point between complete safety and maximum performance
- Add intermediate recovery state before failure

Proposed Workaround:




**Result of enabling workaround:**
**Increased Mean Time Until Passenger Injury** by several orders of magnitude.

Institute for Complex Engineered Systems

GM

Electrical & Computer ENGINEERING

Carnegie Mellon