Elements of Autonomous Vehicle Safety

(The Super-Short Version)

AVS 2018

Prof. Philip Koopman

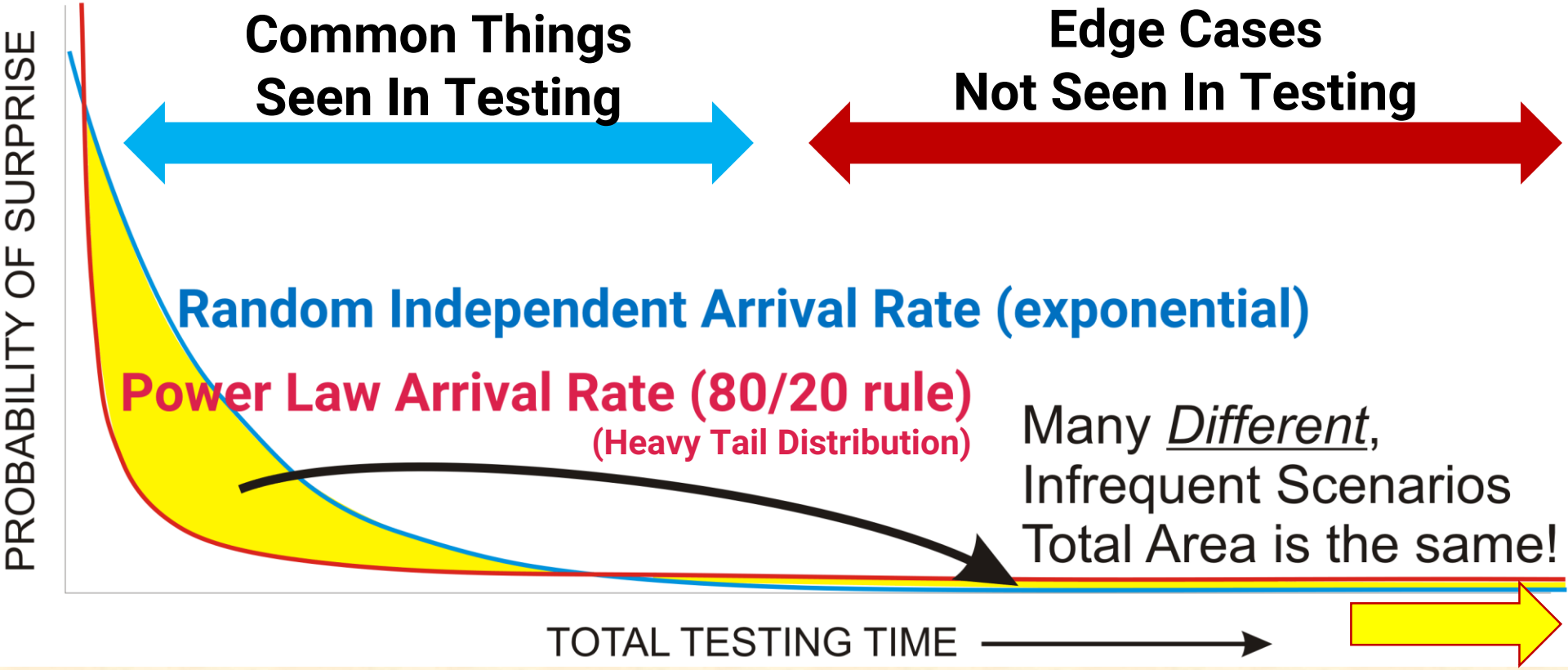
Carnegie Mellon University

SafeAutonomy.blogspot.com

@PhilKoopman

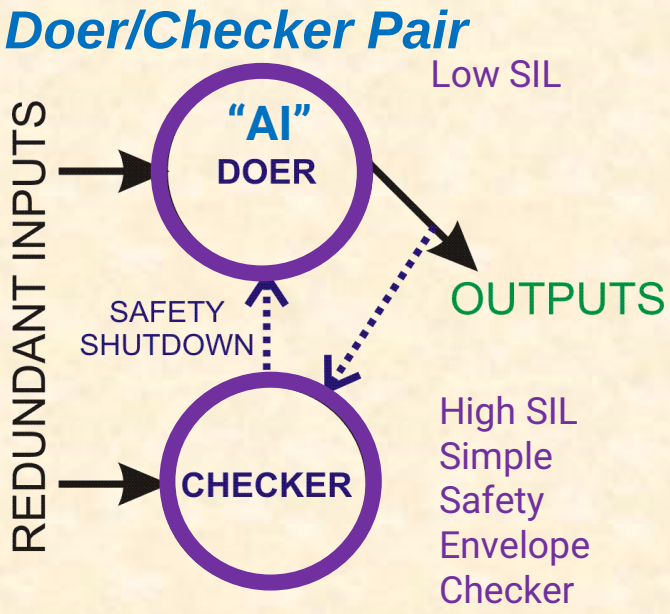
Edge Case Research

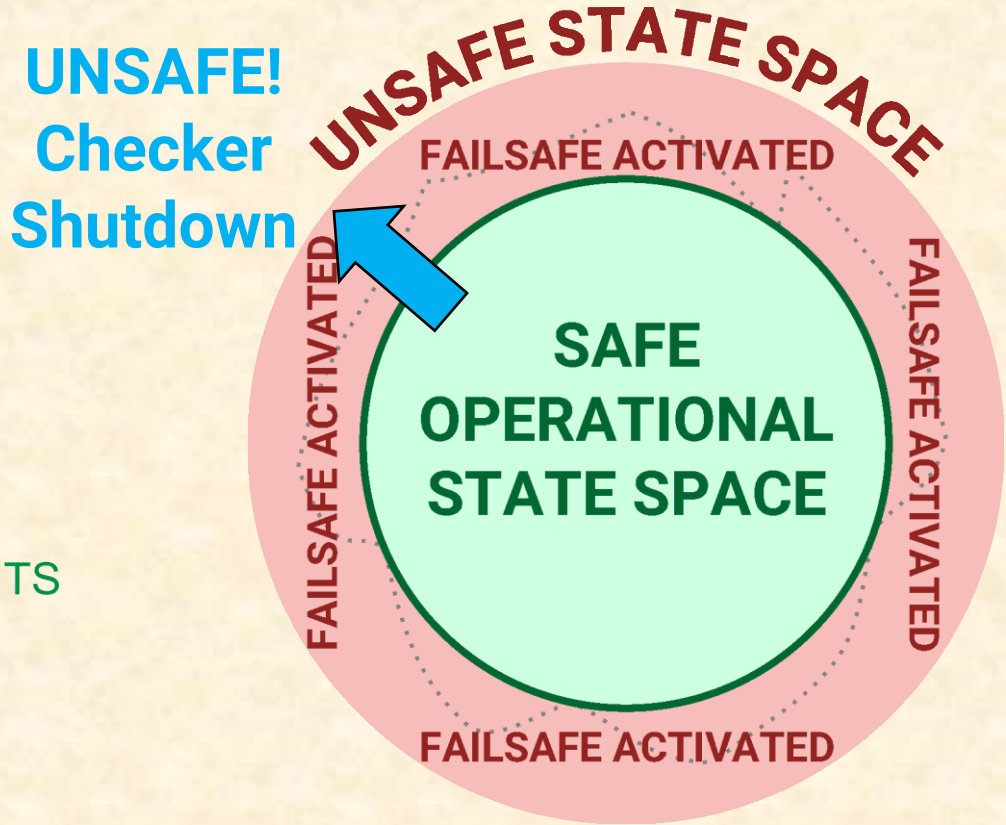
The Real World: Heavy Tail Distribution



Planning and Control: Doer/Checker

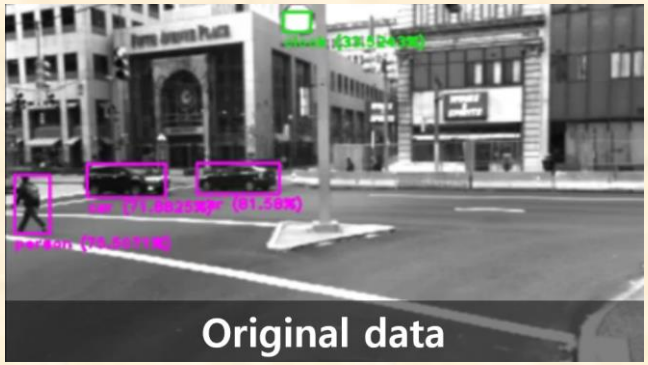
- **Low integrity Doer**
  - E.g., based on training data
- **High integrity Checker**
  - Use traditional safety methods





Perception: Robustness via Augmentation

- Pseudo-realistic degradation
- Move and insert objects



Dark vehicle added to scene

Pedestrian Missed: Gaussian Blur

Pedestrian Missed: Gaussian Noise + Black Car

Other Techniques

- **Conventional V-based software safety**
  - ISO 26262, SOTIF forsafety requirements
- **Rapid safety case update tooling**
  - STPA plus augmented fault trees and GSN
- **Architectural safety patterns**
  - Doer/Checker for a fail silent channel
  - Multi-channel approach for safing mission
- **Robustness/stress testing**
  - Traditional robustness testing
  - Object & event edge case “zoo”

MISSA
AUTONOMOUS SYSTEM SAFETY ACCELERATED

switchboard
RELIABLE SOFTWARE FOR AUTONOMY

hologram
SAFER PERCEPTION FOR AUTONOMY