Industry Methods for Safety Assurance & Testing

Module 3, Lesson 2

UNIVERSITY OF TORONTO
FACULTY OF APPLIED SCIENCE & ENGINEERING

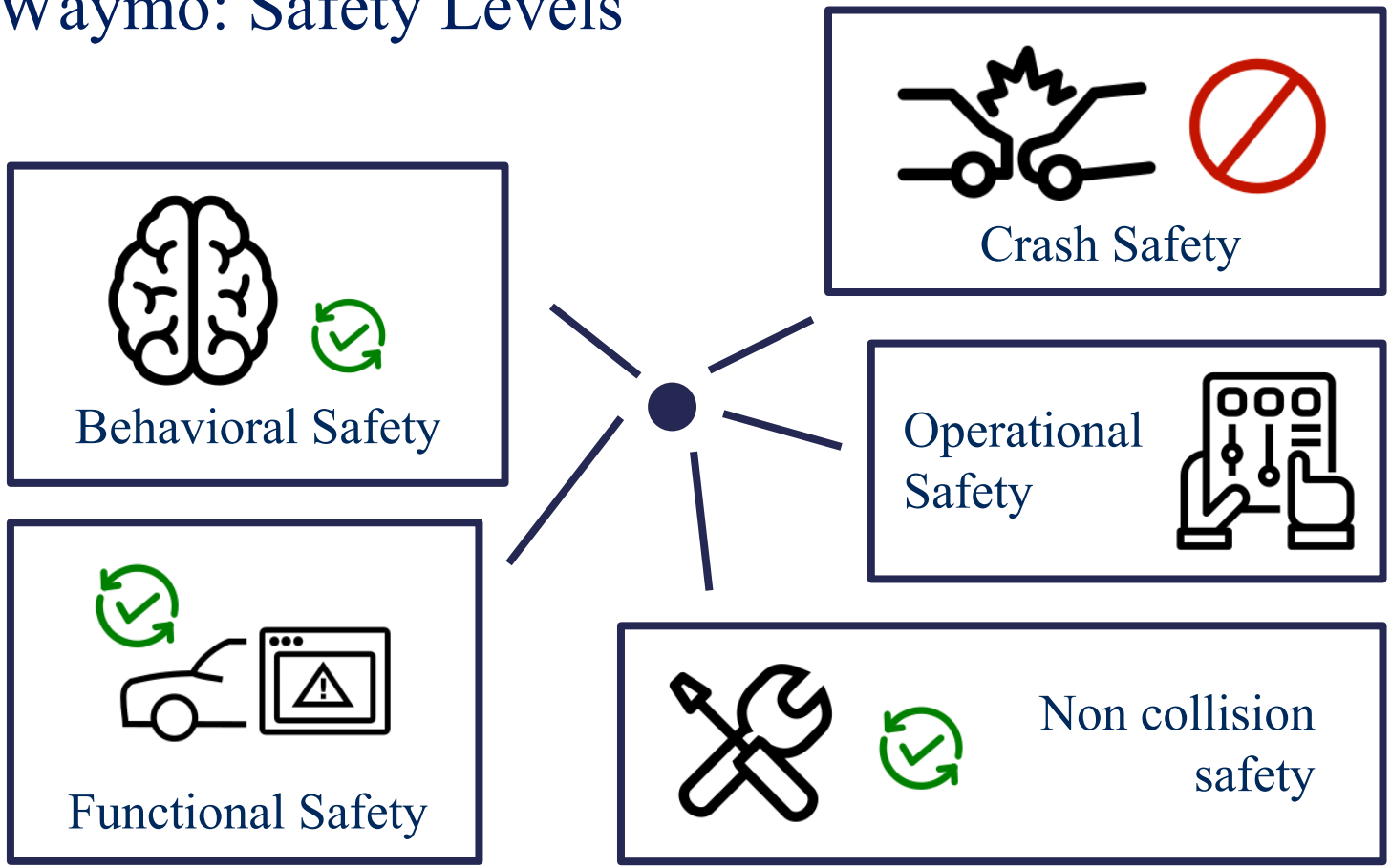
In this video ...

- Industry perspectives on self driving safety
- Approaches to demonstrating autonomy safety

Waymo Safety Perspective

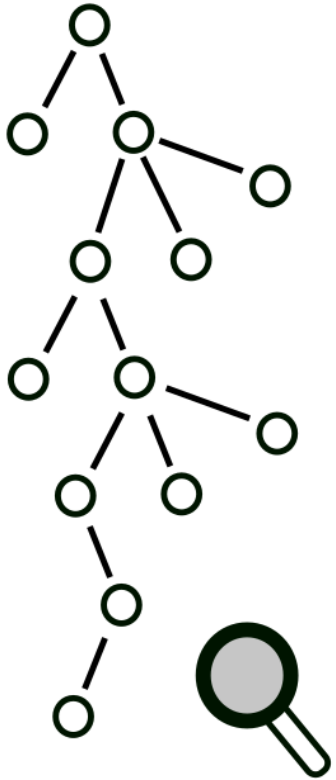
Based on Waymo Safety Report (2017)

Waymo: Safety Levels



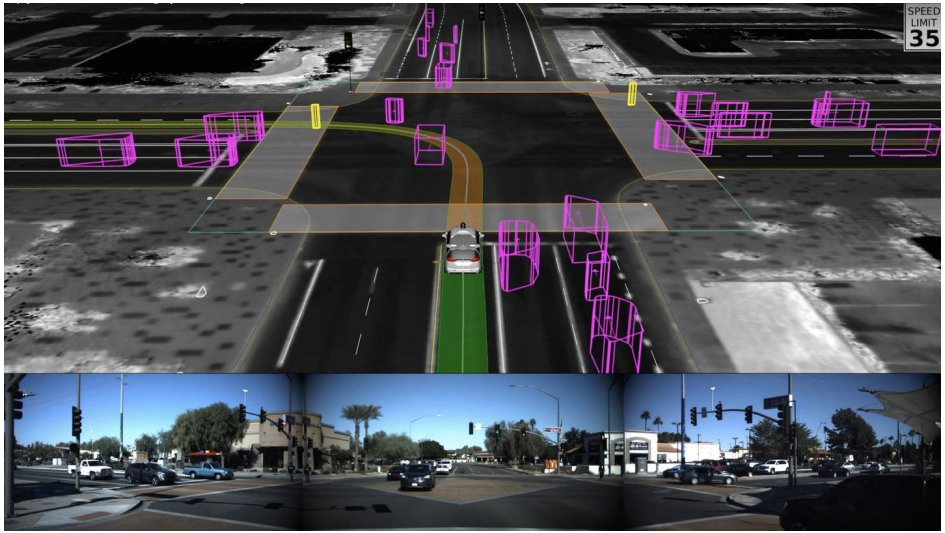
Waymo: Safety Processes

- Identify hazard scenarios & potential mitigation
- Use hazard assessment methods to define safety requirements
  - Preliminary analysis
  - Fault tree
  - Design Failure Modes & Effects Analyses
- Conduct extensive testing to make sure safety requirements are met



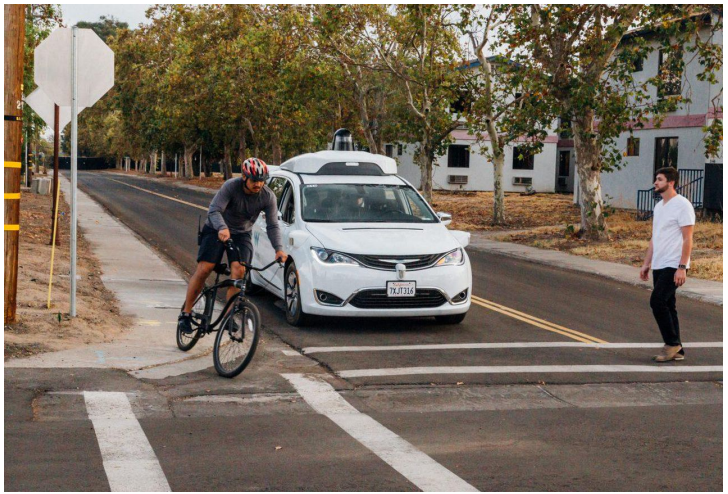
Waymo: Levels of testing to ensure safety

- Simulation testing
  - Test rigorously with simulation, thousands of variations, fuzzing of neighbouring vehicles



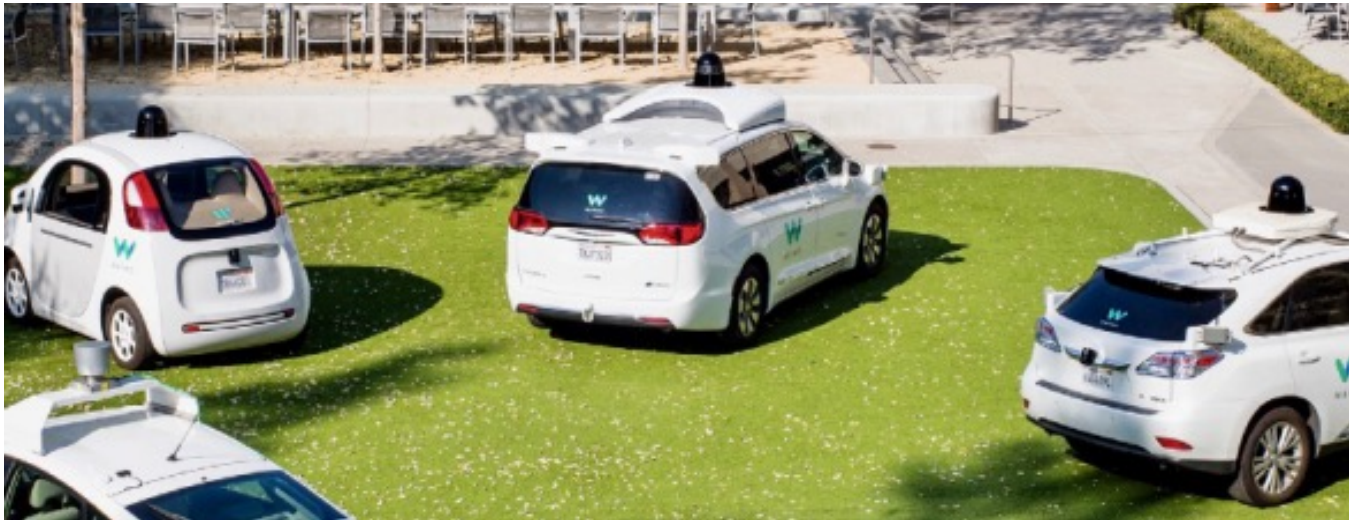
Waymo: Levels of testing to ensure safety

- Closed-course testing
  - Follow 28 core + 19 additional scenario competencies on private test tracks
  - Focus on four most common crashes:
    - Rear-end, intersection, road departure, lane change



Waymo: Levels of testing to ensure safety

- Real-world driving
  - Start with smaller fleet, expand steadily
  - Already testing thousands of vehicles, with more on the way.

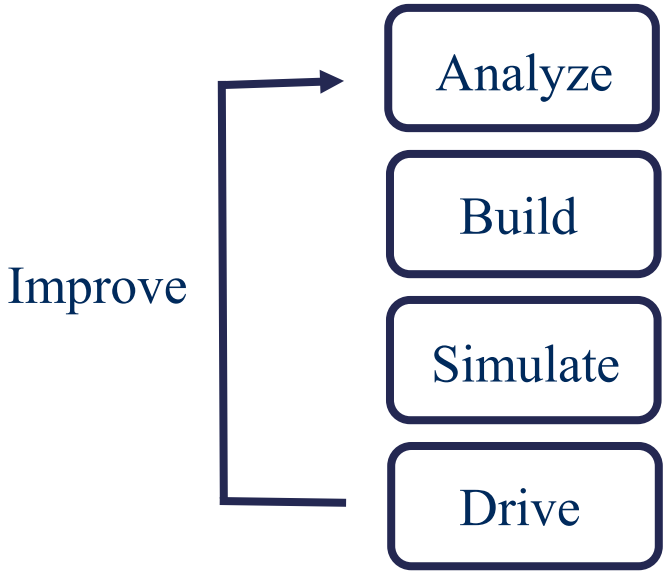


General Motors Safety Perspective

Based on GM Safety Report (2018)

GM: Safety

- Address all 12 elements of NHTSA Safety Framework
- Iterative Design



Control car production!

GM: Safety

- Safety through Comprehensive Risk Management and Deep Integration
  - identify and address risks, validate solutions
  - prioritize elimination of risks, not just mitigation

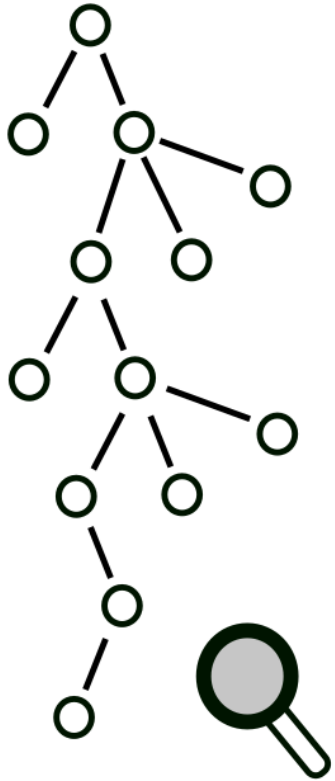
- All hardware, software systems meet
  - self-set standards for performance, crash protection, reliability, serviceability, security, safety
  -

GM: Safety Processes

- **Deductive Analysis**
  - fault tree analysis

- **Inductive Analysis**
  - Design & Process FMEA

- **Exploratory Analysis**
  - **HAZOP**: Hazard & Operability Study



GM: Safety Thresholds

All GM vehicles are equipped with two key safety thresholds:

- **Fail safes** - There is redundant functionality (second controllers, backup systems etc) such that even if primary systems fail, the vehicle can stop normally

- **SOTIF** - All critical functionalities are evaluated for unpredictable scenarios

GM: Testing

- **Performance testing** at different levels
- **Requirements validation** of components, levels
- **Fault injection testing** of safety critical functionality
- **Intrusive testing** such as electromagnetic interference, etc.
- **Durability testing** and **simulation based testing**

Analytical vs Data Driven: Definitions

- **Analytical Safety**
  Ensuring the system works in theory and meets safety requirements found by hazard assessment

- **Data driven safety**
  Safety guarantee due to the fact that the system has performed autonomously without fail on the roads for a very large number of kms

Are autonomous cars safer?

- Driving is still dangerous!
- Car accidents are mostly caused due to human errors (NHTSA Report, 2015)

- In US, on average
  - 1 fatal collion per 146 million km
  - 1 injury collision per 2.1 million km
  - ~ 1 collision per 400,000 km

Critical Reason Attributed to	Estimated	
	Number	Percentage* ± 95% conf. limits
Drivers	2,046,000	94% ±2.2%
Vehicles	44,000	2% ±0.7%
Environment	52,000	2% ±1.3%
Unknown Critical Reasons	47,000	2% ±1.4%
Total	2,189,000	100%

*Percentages are based on unrounded estimated frequencies
(Data Source: NMVCCS 2005–2007)

Are autonomous cars safer?

- Consider California disengagement rates:

- In 2017, Waymo had
  - Driven 563,000 km autonomously in California
  - 63 disengagements
  - 1 disengagement every 9,000 km

- In 2017, GM had
  - Driven 210,000 km autonomously in California
  - 105 disengagements
  - 1 disengagement every 2,000 km

The Dilemma

- **Question**: How many miles (years) would autonomous vehicles have to be driven to demonstrate with 95% confidence their failure rate to within 20% of the true rate of 1 fatality per 146 million km?
- **Answer**: ~400 years, with a fleet of 100 vehicles travelling all the time (total ~8 billion miles)

    - [How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability? (Kalra et al., 2016)]

Summary

- Industry perspectives
  - Waymo - 5 safety levels, processes, testing
  - GM - iterative design, processes, testing
- Data driven safety
  - Disengagement rates and road testing requirements