**Main Cons –** misidentification

**Basic Safety Terms**

***Safety* –** absence of *unreasonable* risk of harm

***Hazard* –** potential source of *unreasonable* risk of harm

**Major Hazard Sources**

***Mechanical Electrical Hardware Software Sensors Behavioral Fallback Cyber***

**Safety Framework**

***Systems engineering approach to safety***

***Autonomy Design – ODD, OEDR, Fallback, Traffic Laws, Cybersecurity, HMI***

***Testing & Crash Mitigation – Testing, Crashworthiness, Post crash, Data recording, Consumer Ed***

**Safety**

Some Industries: *Waymo* and *GM*

*NHTSA concepts 12 rules (Waymo covers all)*

**Waymos Safety System:**

1) Behavioral Safety (traffic rules, a wide range of scenarios within the ODD, maintain the safety through it)

2) Functional Safety (backups and redundancies to switch to the previous version of model)

3) Crash Safety (design for the minimum damage at crash)

4) Operational Safety (UI friendly and usable)

5) Non-collision safety (responders, mechanics, hardware engineers...)

Analysis:

Preliminary

Fault Tree

Design Failure Modes and Effects

**Closed-course Testing**

28 core + 19 additional private test tracks

Most common 4 crashes (84% of all the crashes):

Rear-end

Intersection

Road Departure

Lane Change

Real-word driving

**GM Safety System:**

*NHTSA concepts 12 rules (Waymo covers all)*

Iterative Design

Improve:

Analyze

Build

Simulate

Drive

Inductive Analysis:

Full control of the hardware as they are the developers of the hardware themselves!

Exploratory Analysis:

HAZOP: Hazard and Operability Study

**Safety Threshold:**

***Fail Safes***

***SOTiF***

***Performance testing***

***Requirements Validation***

***Fault injection testing***

***Intrusive testing***

***Durability testing and simulation based testing***

***Analytical Safety***

Theory safety

Data driven safety

**Probability Calculation**

OR:

A + B

AND:

A \* B

**HAZOP - a variation on - FMEA**

Qualitative brainstorming process, needs “imagination”

Uses guide words to trigger brainstorming (not more, less, etc.)

Applied to Complex processes:

Sufficient Design information is available, and not likely to change significantly

**Final RPN List:**

Control Failure

GPS Failure

Motion Prediction

Sign Prediction

**ISO 26262 – Functional Safety Standard**

**ISO/PAR 21448.1 – Safety Intended Functionality**

Functional Safety is defined as:

Safety due to absence of unreasonable risk

Only concerned about malfunctioning system