Man Machine or In Between

Investigations Involving Advanced Driver Assistance Systems (ADAS)


Mountain View, CA, NTSB HWY18FH011

Robert L. Swaim

Founder and Contact: www.HowItBroke.com

NTSB Engineering National Resource, Aviation Systems - Retired

HowItBroke.com

Bob Swaim

NTSB Aviation Major Accident Investigator since 1987

- Autopilots and aircraft systems

2013 Launch investigator for JAL 787 fire investigation

- Lithium-Ion battery work at UL labs, vehicle, and battery manufacturers

Electric vehicle investigator since 2017

SAE EV SME, Instructor, and J2990 First Responder Safety Committee

NFPA EV SME, Instructor


2017 Lake Forest, CA


B737 Autopilot mis-use


Mid-air collision B757 & Tu-154

Photo courtesy of the San Jose CA Fire Department

HowItBroke.com

Majority of accidents result in no injuries
Most of public is never aware

While some accidents do result in injuries

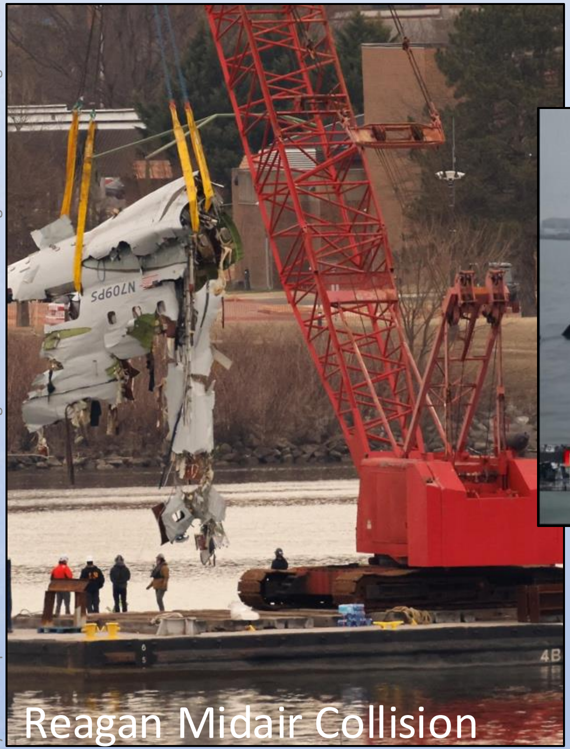
"That can't happen" or "It doesn't work that way"

Usually said by the Design Engineer

Addis Ababa, Ethiopia

Hudson River Helicopter

Gaithersburg, MD


Reagan Midair Collision

Aviation Has Had Numerous Autopilot Involved Accidents To Learn From

Boeing 737 MAX, Ethiopian flt 302
Ethiopia, March 10, 2019, 157 fatal

Boeing 737 MAX, Lion Air flt 810
October 29, 2018, 189 fatal

AOA sensor failure coupled with design error and training leading to improper pilot responses

Boeing 777, Emirates flt 521
Dubai, August 2016, 1 fatal, 38 injured
Pilot expected go-around thrust not realizing ground contact changed flight mode

Airbus A330, Air France flt 447
Atlantic Ocean, June 1, 2009, 228 fatal
Ice in airspeed probe led to pilot errors

Boeing 737-800, Turkish flt 1951
Amsterdam, February 25, 2009, 9 fatal, 120 injured
Radar altimeter input error and Boeing vs Airbus training differences

Boeing 737-800, Kenya Airways flt 507
Douala, May 5, 2007, 114 fatal
Lack of feedback that autopilot had not engaged when expected to

From Only These Six:
735 fatal, 158 injured

Triple redundant systems in aviation - yet ...

...loss of control found in 43% of 2010-2014 fatal commercial accidents (37)

The #1 Autopilot related cause of accidents is human interface

Typically perception of autopilot performance was not what was expected

The #2 Cause was pilots disconnecting or getting "behind" the airplane

"What's it *[the autopilot]* doing now?"

Common airline crew saying

"Disappointment *[causing stress and errors]* is **the gap that exists between our expectation and reality"** – Maxwell

Our goal is to not let reality differ from expectations

Accident investigations provide the ultimate test and judgement

Numerous ways to define “safety”

Dictionary:

The state of being safe; freedom from the occurrence or risk of injury, danger, or loss.

The quality of averting or not causing injury, danger, or loss.

The action of keeping safe.

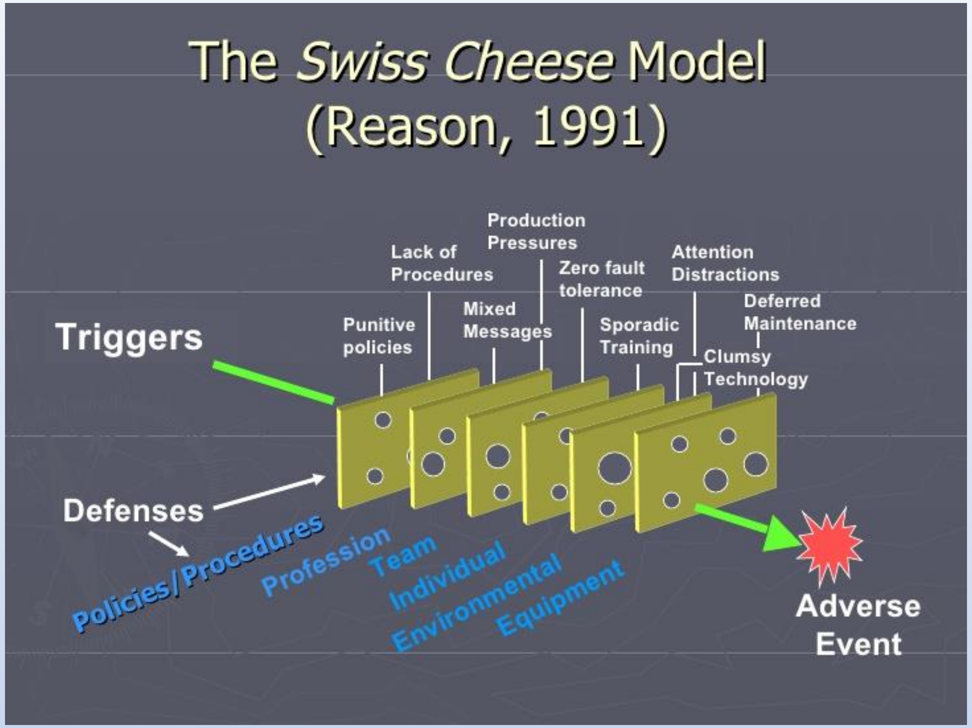
Traditions, Established codes or standards, Regulations,

Statistical definitions: *(per FAA Regulation 49 CFR Part 25.1309)*

(1) Probable failure conditions cause loss at a rate of less than $1x10^5$
(2) Improbable failure conditions between $1x10^5$ and $1x10^9$
(3) Extremely Improbable failure conditions are $1x10^9$ or less

Note: Transport airplanes are designed to a minimum of Extremely Improbable

Numerous ways to define "safety" and risk prevention



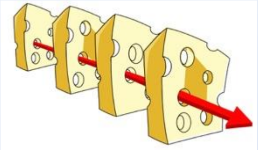
Chain model that anything is only as strong as weakest link:

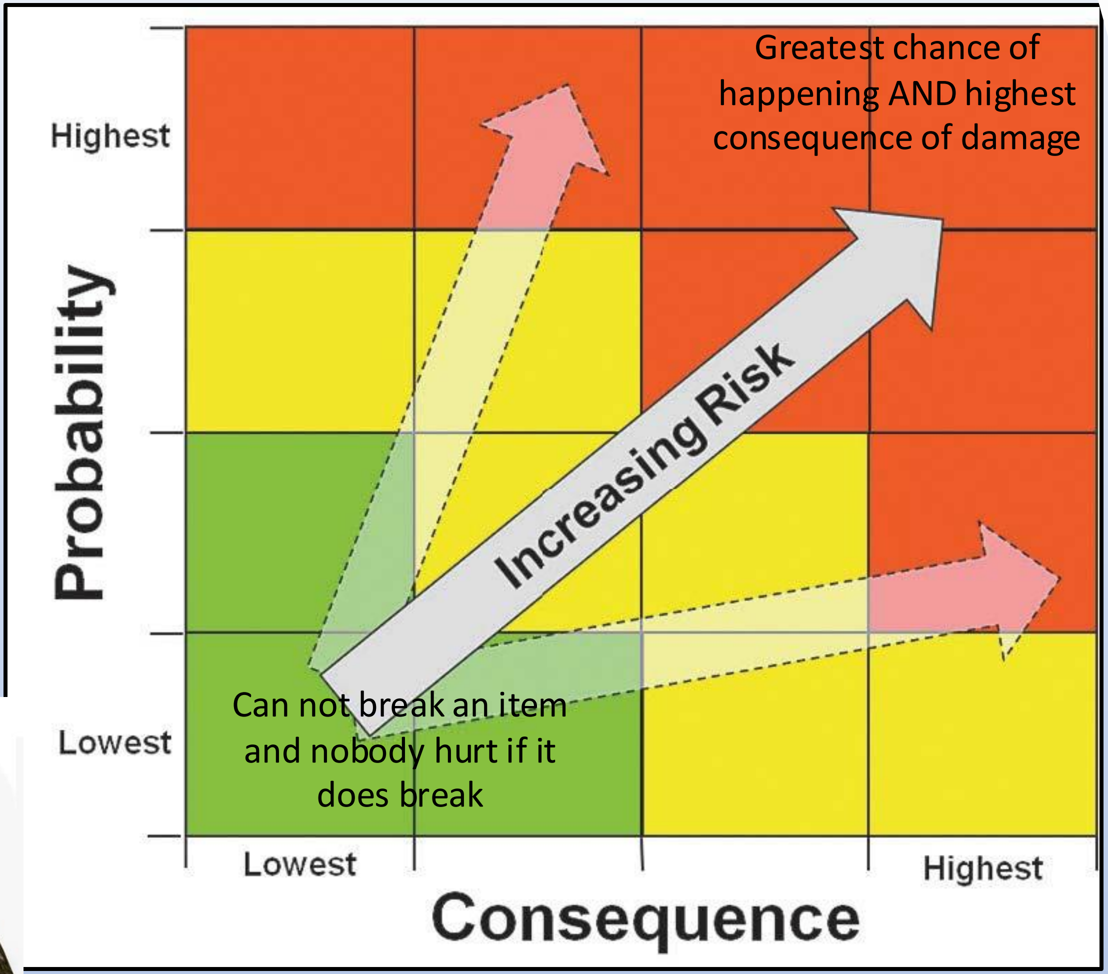
But the 5 M's of Deming always apply:

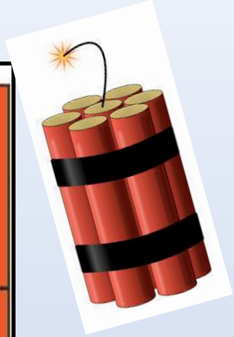
Man
Material
Machine
Method
Measurement

Plus Environment

Safety definitions
Risk defined by failure probability and consequence

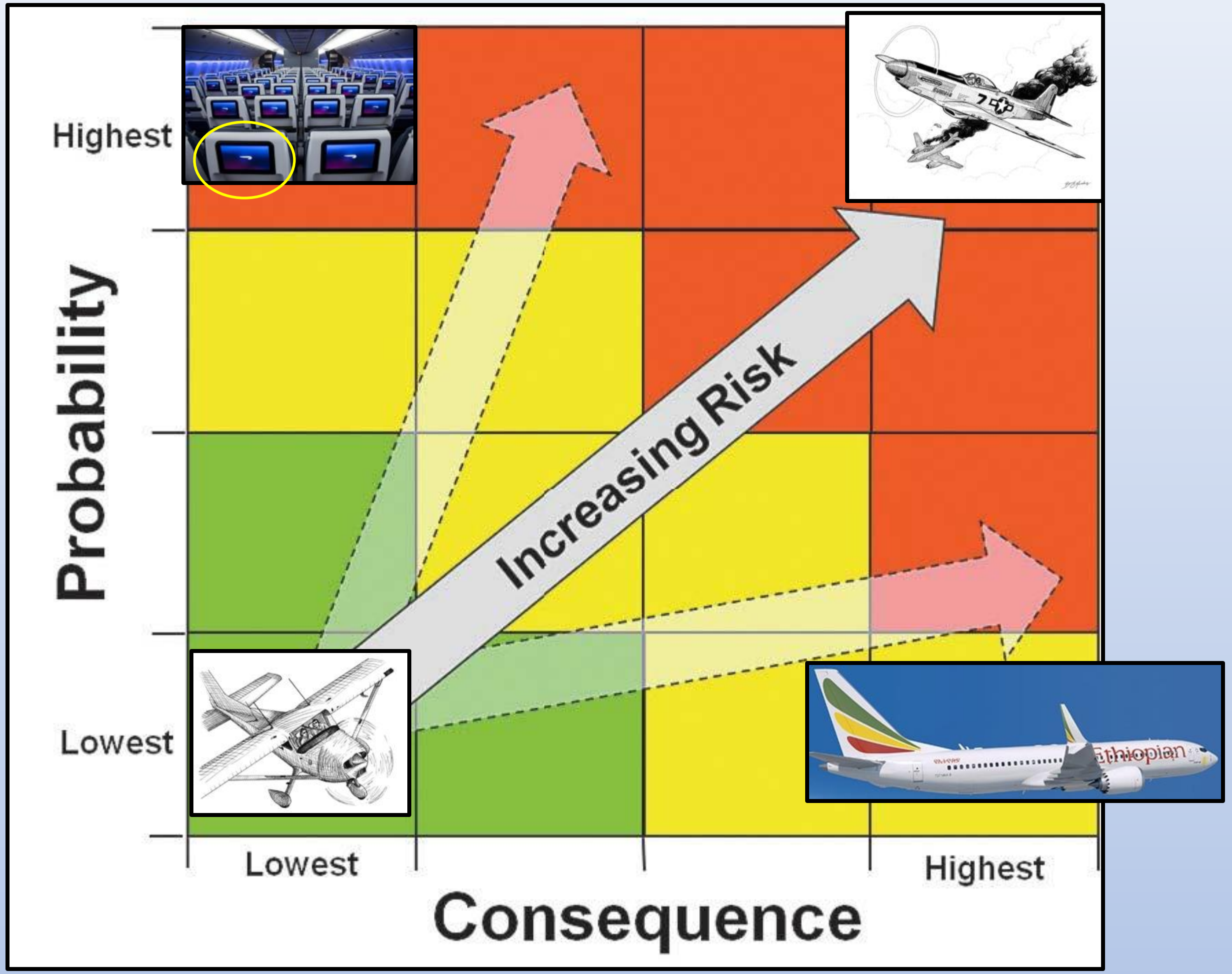






HowItBroke.com

Failure is accepted with various levels



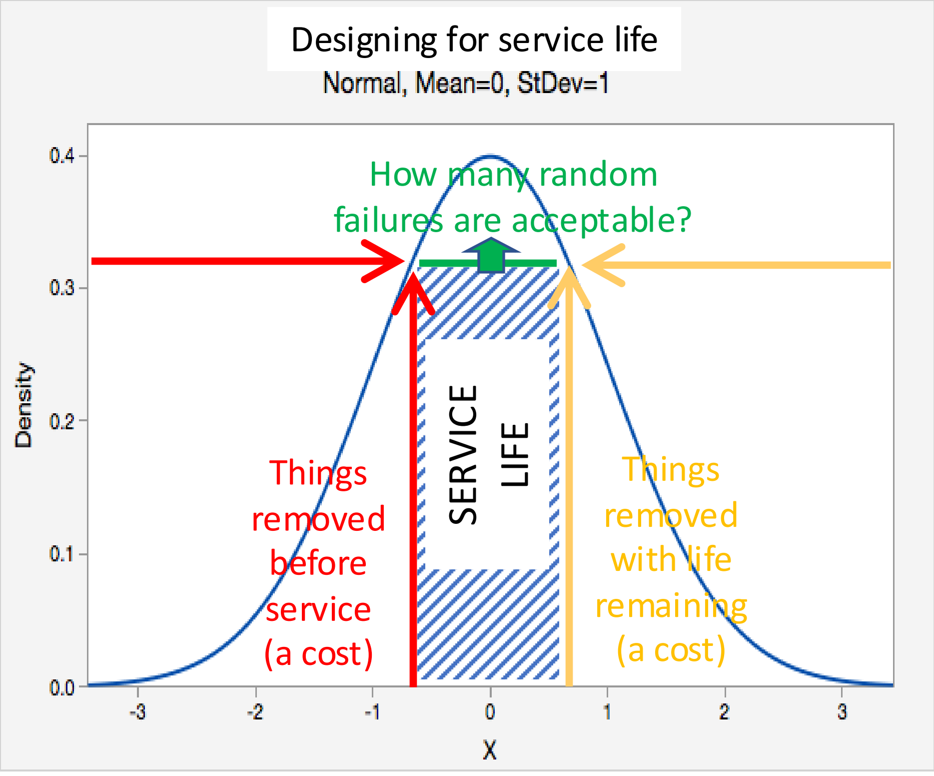
Defining risk and achieving design goals

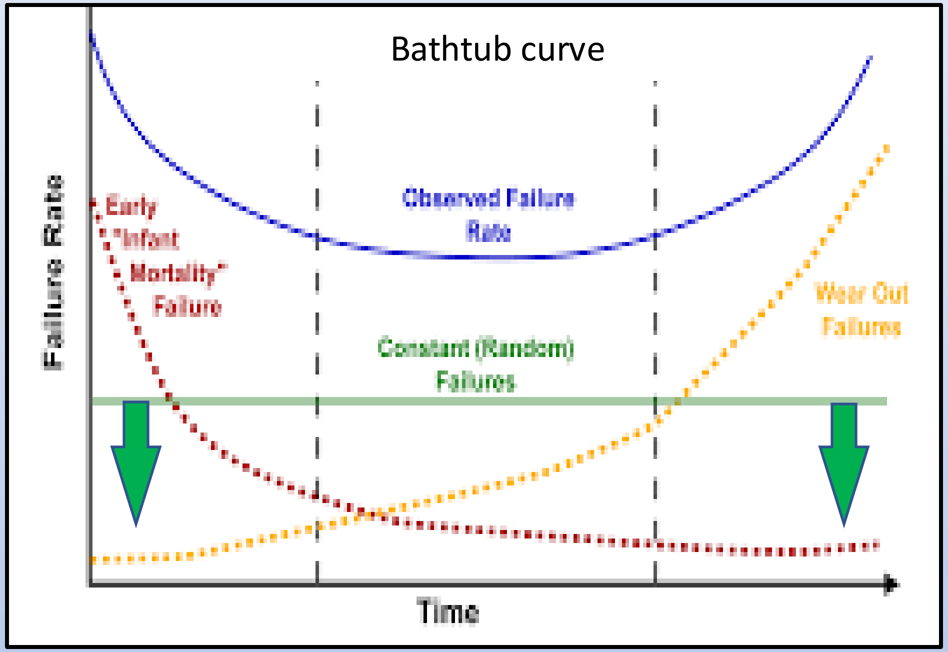
Identify acceptable failure rate

Design standards, pre-test, burn-in, etc address infant mortalities

Maintenance, repair, or replacement remove wear-out failures.

How to reduce random failures?

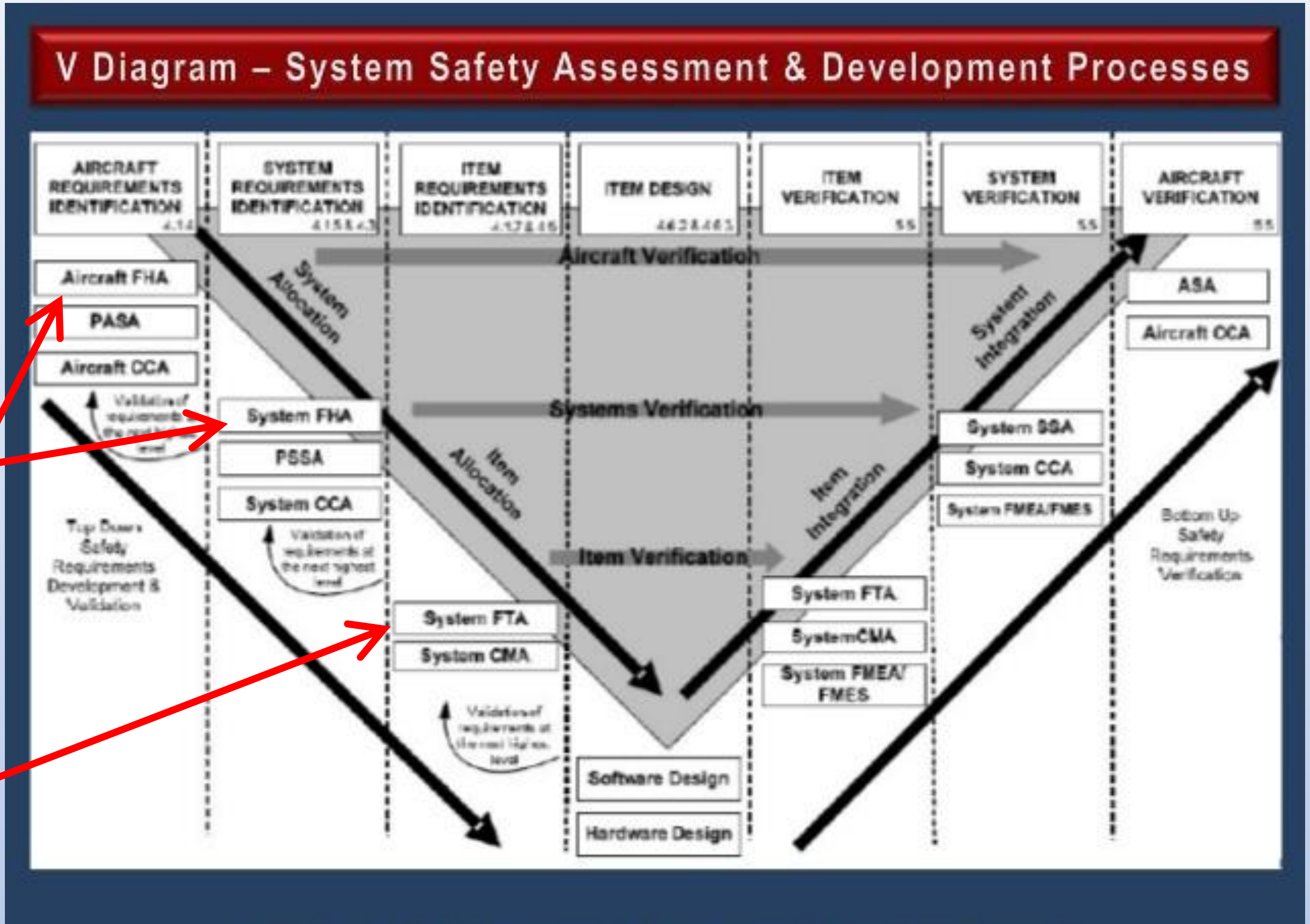




HowItBroke.com

Before design risk levels are established

Basis for calculations established on other designs



Source: ARP 4754 - Guidelines for development of civil aircraft systems

Functional Hazard Assessments defne acceptable levels

Detailed fault tree analysis

$$RF = P_f + C_f - (P_f)(C_f)$$

HowItBroke.com

Before design risk levels are established

Basis for calculations established

Risk Factor are derivatives of Probability and Consequence

Remember Extremely Improbable failure conditions of $1x10^{9}$ or less?

Risk Factor =

$$\text{Risk Factor} = \underbrace{P_f = \frac{\sum_{n} P_i}{n}}_{\text{Probability}} + \underbrace{C_f = \frac{\sum_{m} C_i}{m}}_{\text{Consequence}} - \left(\underbrace{P_f = \frac{\sum_{n} P_i}{n}}_{\text{Probability}} \times \underbrace{C_f = \frac{\sum_{m} C_i}{m}}_{\text{Consequence}} \right)$$

n = Number
Of components?
Of flights?
Of on/off cycles?
(etc)

First place to look

for errors is $\underline{n}$!

HowItBroke.com

What Is An Investigation?

Definition and scope depends on purpose and audience

To the Police officer

When scene is documented, damage recorded, interviews complete, review for traffic violations

To the accident investigator

Probable Cause is established after developing fact based analysis

To the engineer

Review for failure and design corrections

To the lawyer

Collection of potential monetary damage

All Investigations Follow Time-Proven Process

FIRST – Understand who has **jurisdiction** and responsibility **to lead** the investigation?

(Investigator In Charge, IIC)

Four types of investigation are:

Criminal - Government
Safety - Government
Civil – Litigation about monetary damages between individuals &/or companies
Technical – Typically manufacturers

Government has first rights, especially with fatalities
Companies support Government
Government must recognize proprietary needs of companies

SECOND – Leadership must agree on process or how to refine to circumstances

THIRD – Gather facts BEFORE analysis

Differences Between Facts, Analysis, Findings, and Probable Cause

FACTS	ANALYSIS	FINDINGS	PROBABLE CAUSE
Documentation of:	Only after facts collected:	What specific factors led to the accident	Short statement
Physical evidence Maintenance records Phone records Medical records Weather conditions Interview statements etc	Comparison of facts such as Physical evidence vs maintenance records Comparing Interviews etc	Define what was not involved If this Then that	The accident was caused by an inattentive driver and design unable to …

Collect Factual Data By Breaking Into Focal Groups

Groups work in defined focal areas, such as:

- Driver and human factors
  - People involved, their training, and backgrounds
- Vehicle(s) and systems design,
  - Previous similar events,
  - Maintenance records,
- Roadway, including barriers, markings, etc
- Weather and other environmental factors,
- Traffic, communications, radar or other recordings,

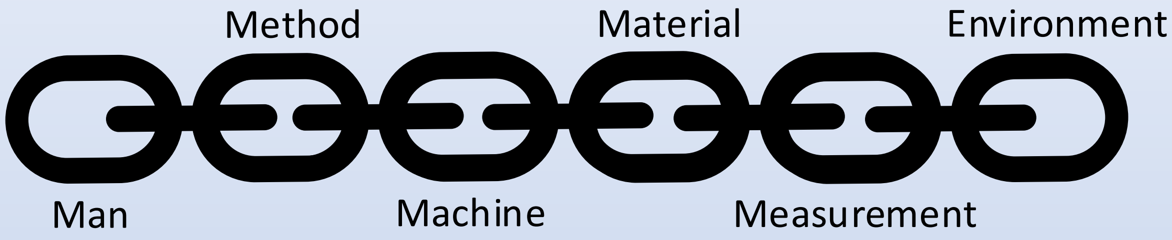
2017 Mountain View, California

Conduct daily organizational meetings

Share factual findings with other groups and leadership

Use Demings “Five M’s and E” As **<u>The Facts To Look For</u>**

The factual links used to document a causal chain.

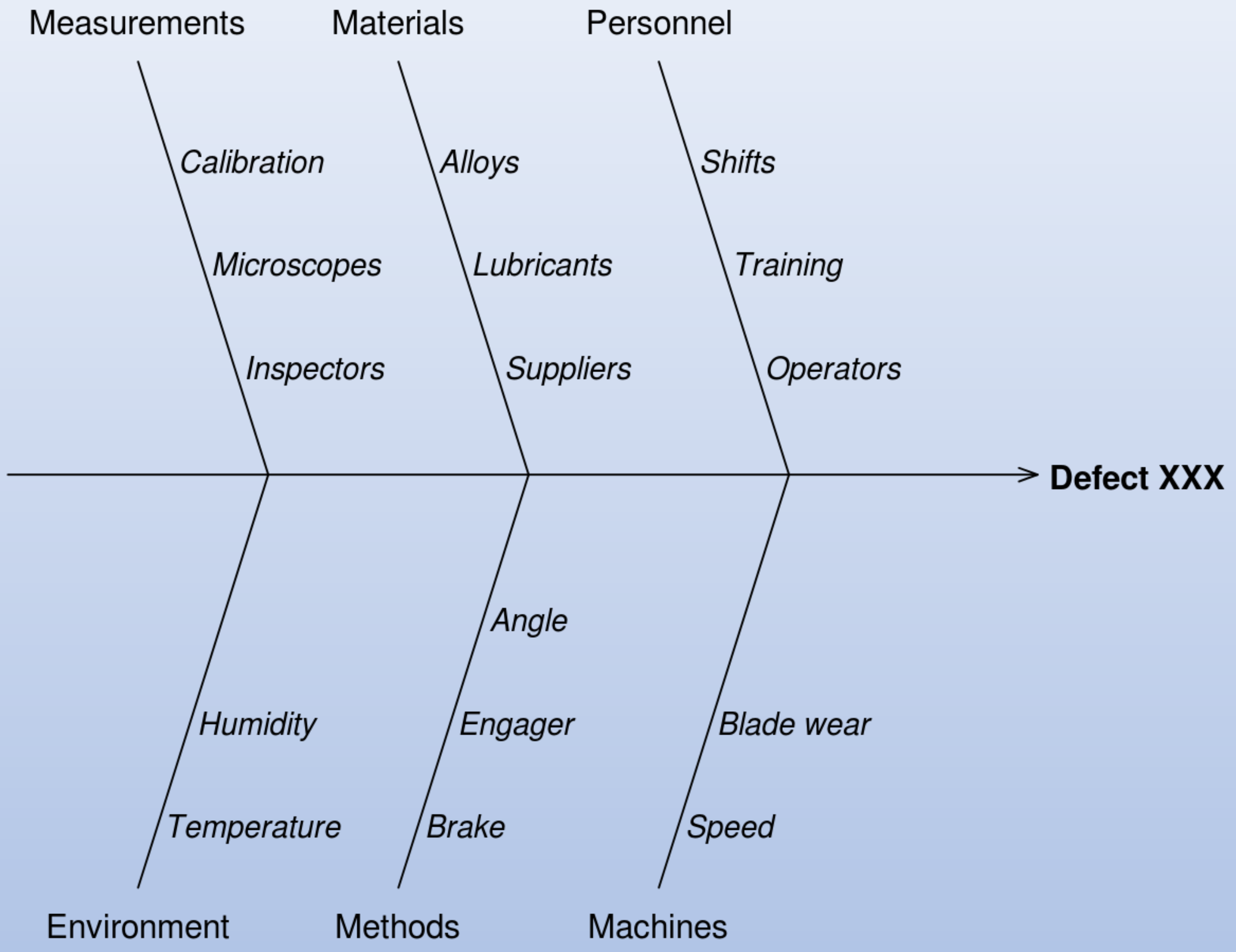


Numerous Ways To Categorize And Record The Facts Found

Still valid method adapted from 1920s Ishikawa "Fish Bone" diagrams

The 5 Ms & E:

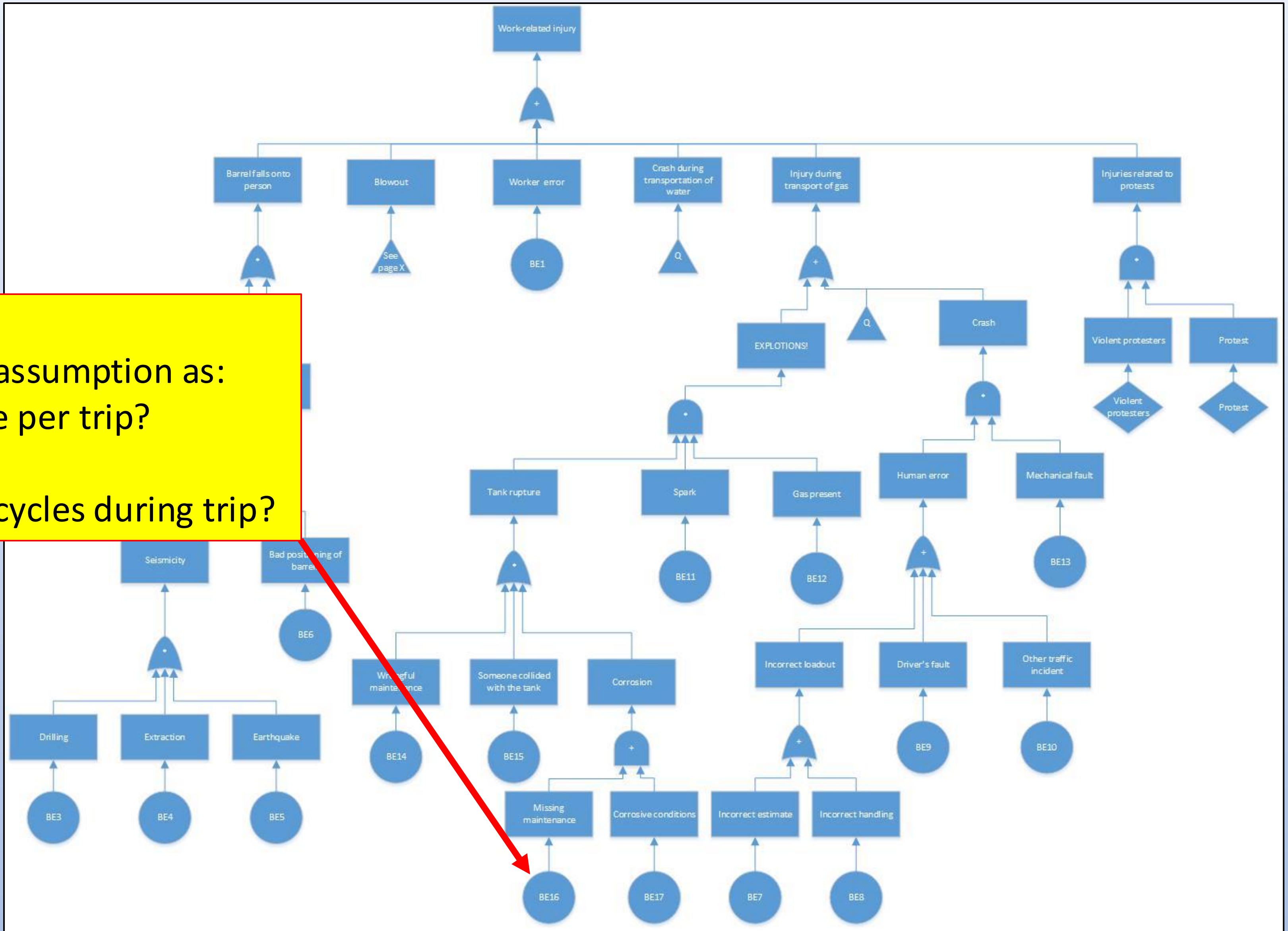
- Man
- Machine
- Method
- Material
- Measurement
- Environment



Software Based Logic Fault Trees Are Needed In Complex Investigations

Risk analysis software tools can have thousands of cells

Due to compounding of errors, **increasing the number of cells results in decreasing validity**



BEWARE!!!
Count a basic assumption as:
One occurance per trip?
or
Thousands of cycles during trip?

Source: http://wiki.doing-projects.org/index.php/Fault_tree_analysis

Summary: Various Investigation Processes Exist & Most Have Validity

Simplest is to keep asking factual "Why?"

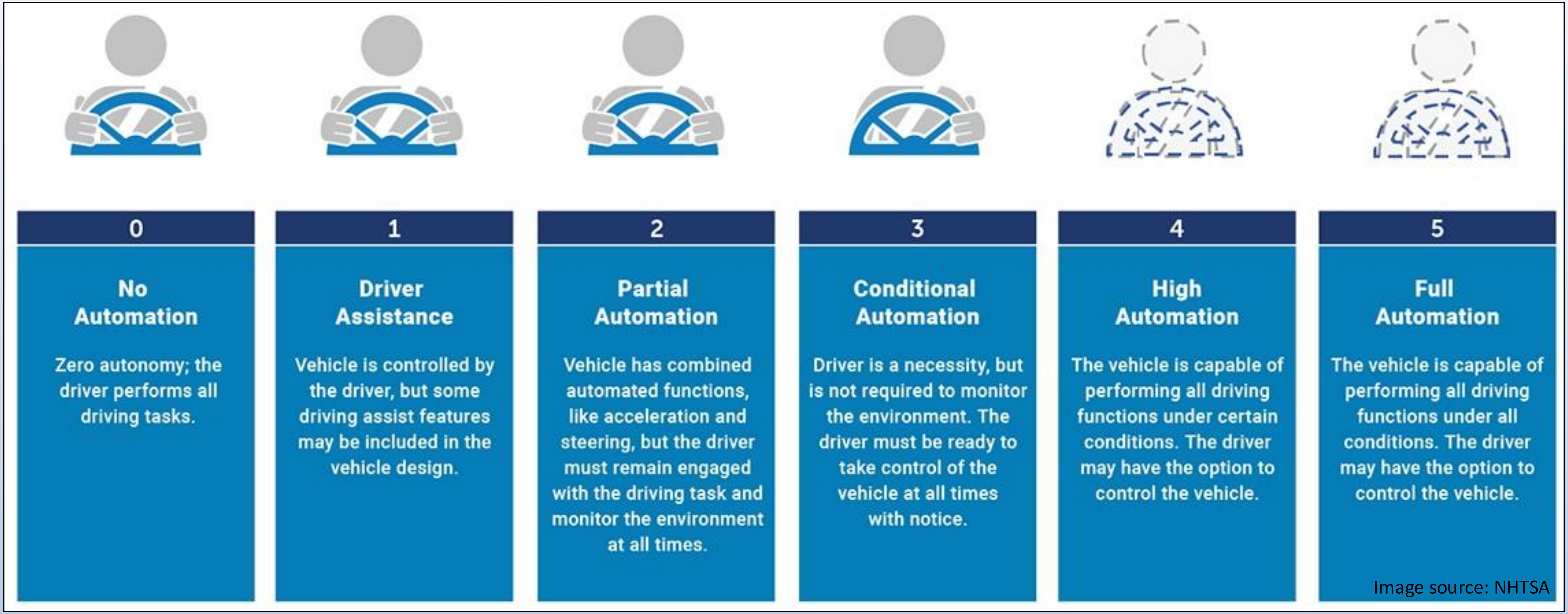
5 Why Method:
Why – Battery is dead
Why – No charge system output
Why – Alternator belt broken
Why – Belt worn to failure
Why – Inadequate maintenance

Too simplistic for most problems

Advanced Driver Assistance Systems (ADAS)

Levels Of Advanced Driver Assistance Systems (ADAS)

SOCIETY OF AUTOMOTIVE ENGINEERS (SAE) AUTOMATION LEVELS

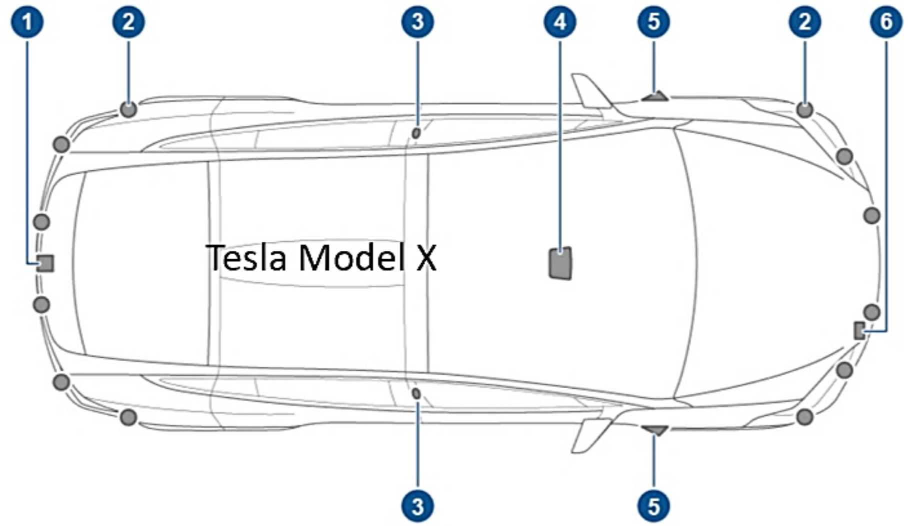


SAE J3016 and ISO 22736 Contain definitions for features and levels of control

Sensors – Tesla Model 3 Cameras, Radar, Ultrasonic Locations

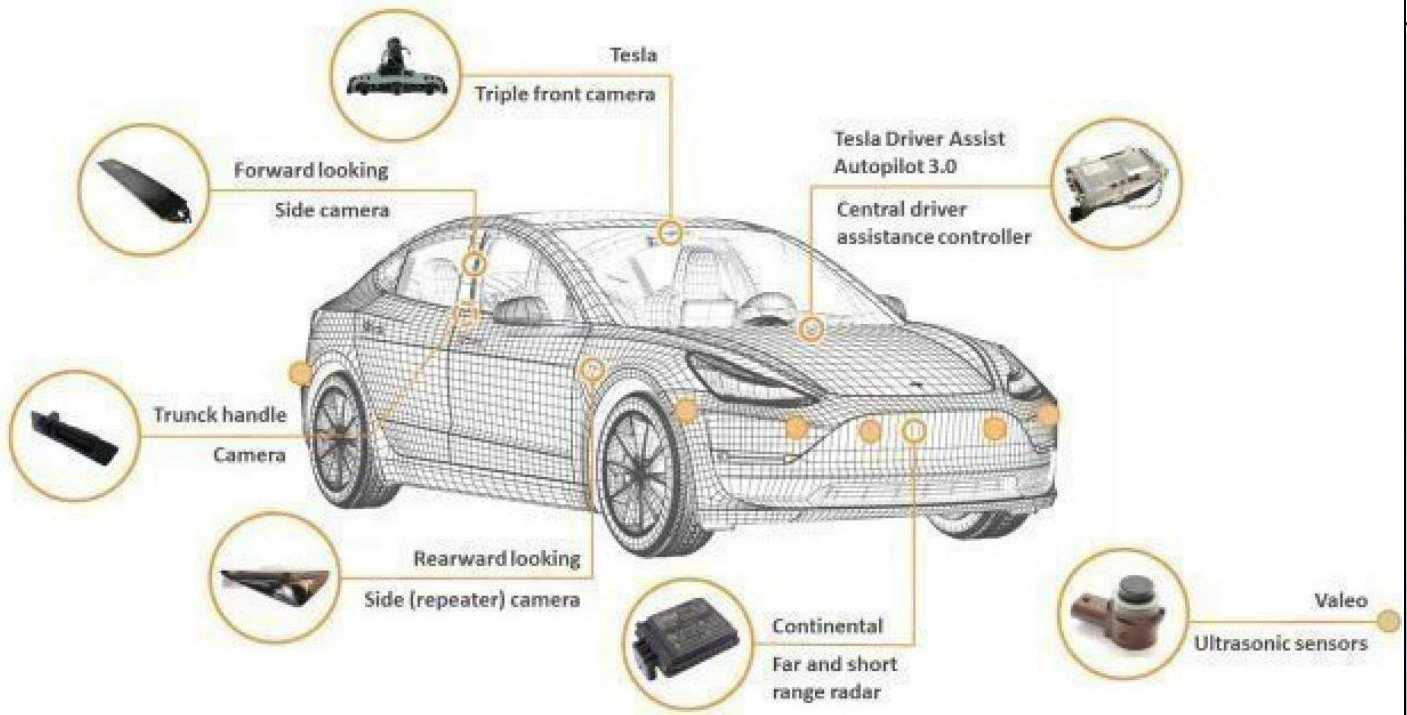
Standard – ADAS Level 2
Autopilot

Paid – ADAS Level 3
FSD Full Self Driving



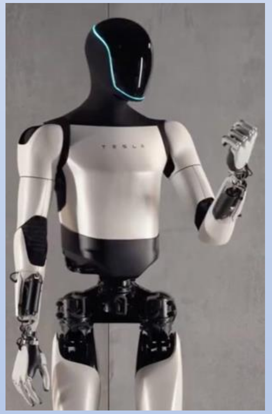
1. Camera mounted above the rear license plate
2. Ultrasonic sensors in front and rear bumpers
3. Camera mounted in each door pillar
4. Three cameras mounted above rearview mirror
5. Camera mounted to each front fender
6. Radar mounted behind front bumper on right side

Ultrasonics removed post 2022



Ultrasonics detect objects with sound waves
Better for near objects such as curbs
Affected by weather

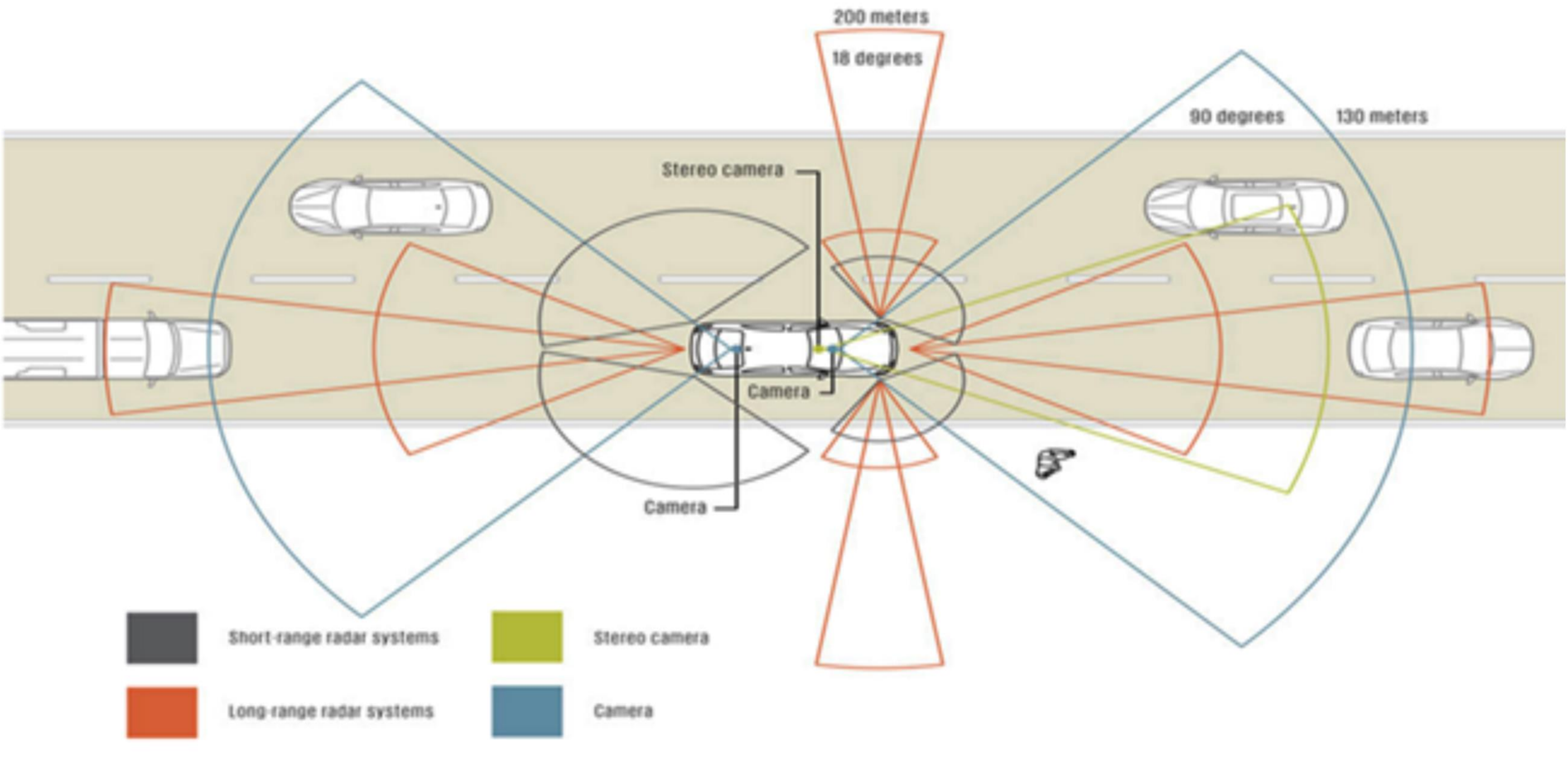
Radar detection with radio waves.
Wider and longer detection ranges



8 Cameras

HowItBroke.com

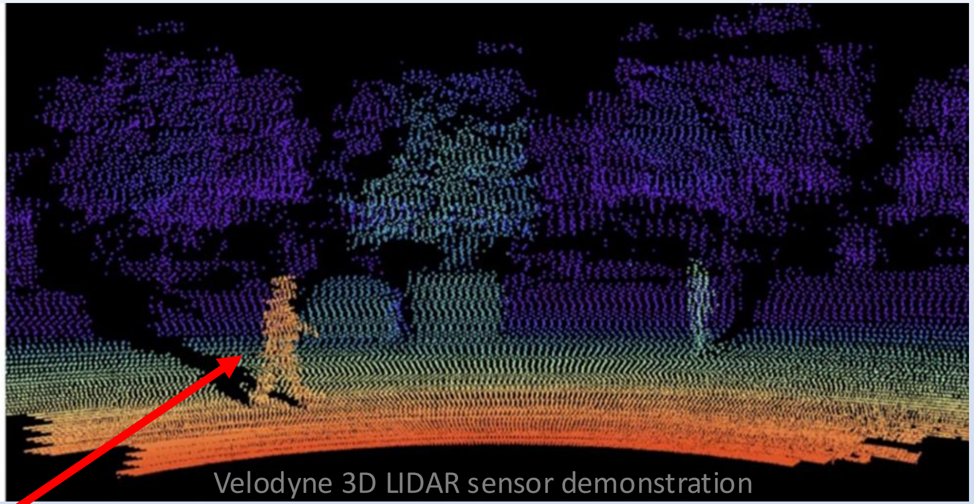
Sensors – Tesla Model 3 Cameras, Radar, Ultrasonic Functions



Sensors of different capabilities cover 360 degrees, with overlapping fields of view.

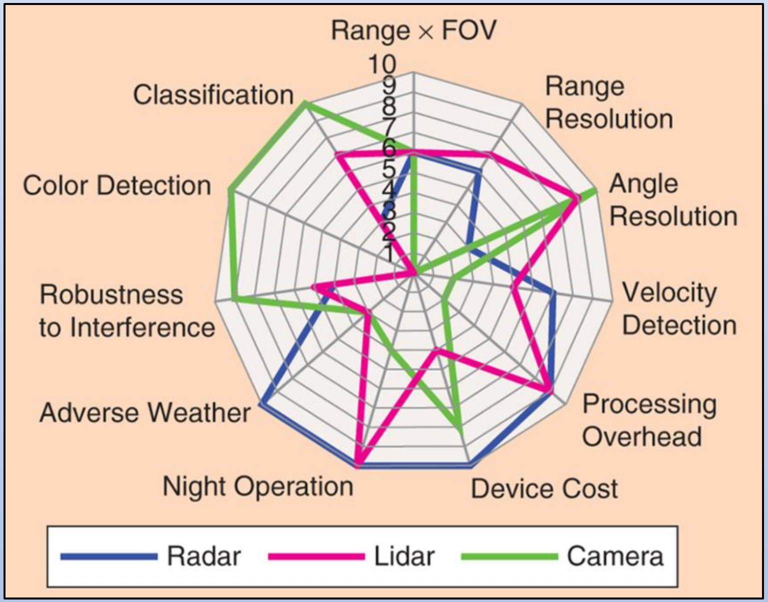
Sensors - Light Detection And Ranging (LIDAR)

Integrates With Cameras and Radar



2017 $75,000
2022 $ 6,000
2025 $ 400

Performance Compared Under Specific Conditions	Camera	RADAR	LiDAR
Dark, Little to No Light	Will Not Work	Very Good (Not Effected by Light Conditions)	Very Good
Variable Lighting Condition	Blinds the Camera	Very Good (Not Effected by Light Conditions)	Very Good
Adverse Weather (Rain, Snow and Fog)	Shortens Range	Very Good	Shortens Range
Angular Resolution	Poor at Long Range	Currently (2-5 Deg) Developmental (0.5-1 Deg)	0.1 Degree
Color & Contrast	Yes	No	No Color, Limited Contrast Info
Cost of Today Technology	2 Mega Pixel Resolution (Low Cost)	24/77 GHZ RADAR (Medium Cost)	Commercialized LIDAR System (Higher Cost)



HowItBroke.com

Alphabet (Google) – Waymo ADAS Level 5

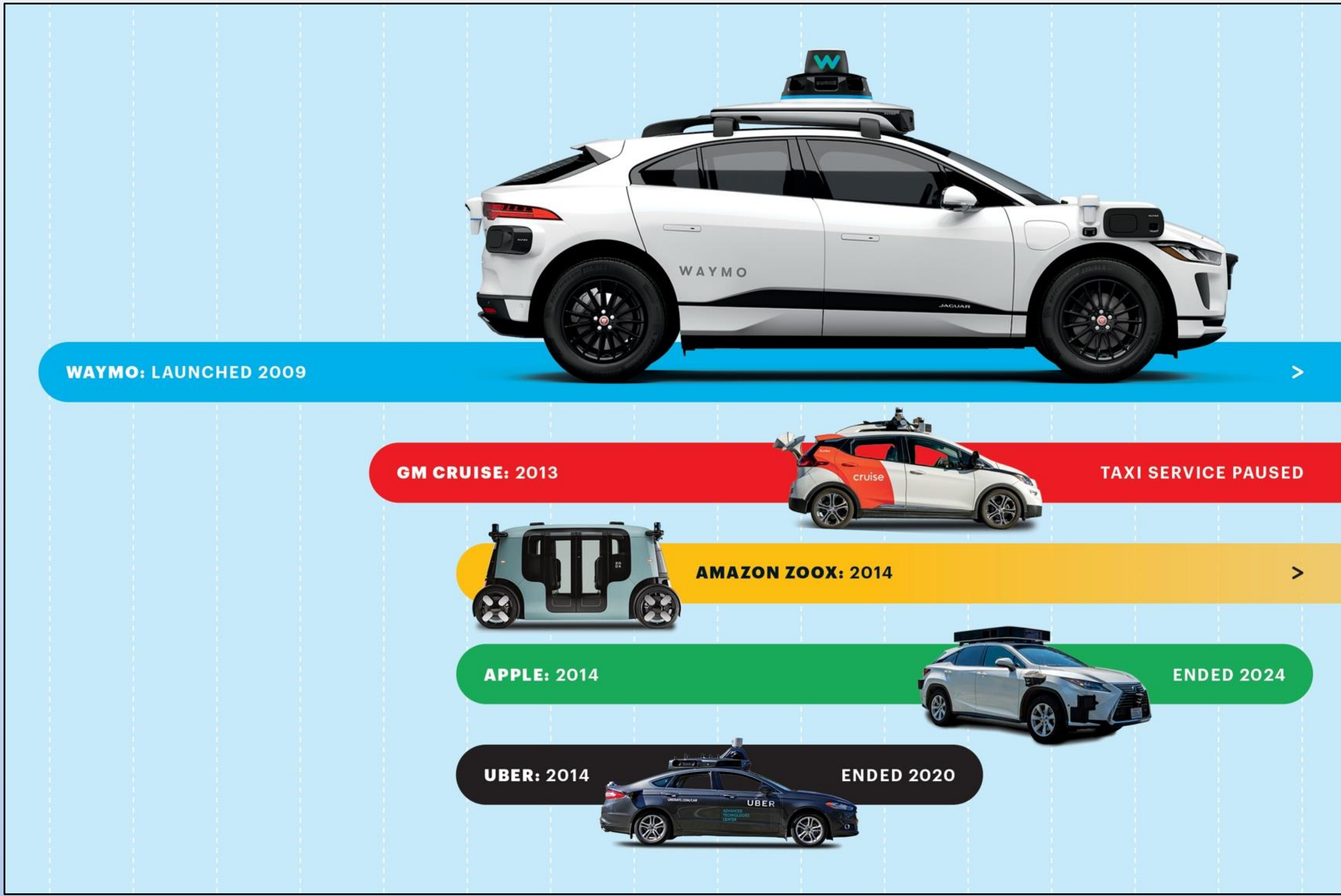
Based in LIDAR, cameras, short & long radar, ultrasonics

Tested in 15 States.

Geo-fenced to San Francisco, LA, Phoenix

Draws on 40 millions miles experience,

20+billion simulation miles



Compared to all traffic:

83% Fewer airbag deployment crashes,
81% fewer injury crashes,
64% fewer police reported crashes

HowItBroke.com

Tesla Robo Taxi – Attempting ADAS Level 5

Pros:

- Based in cameras, short & long radar, ultrasonics
  - Similar to Model 3 & Y
- Extremely limited intro geo-fenced to Austin TX
- Draws on millions of miles experience in S, 3, X, Y
  - Already mapped roads and conditional variations

Potential drawbacks:

- Sensors not optimally placed to see traffic
  - (Situational awareness)
- Camera based system is sensitive to quality of road markings
- Lack of method to keep camera and other inputs clean
- LIDAR spotted on test vehicles

Comparative Records

Tesla – Many more miles driven without geo-fencing

(Data since 2019)

736 crashes

17 fatalities

WAYMO – 40 million geo-fenced miles

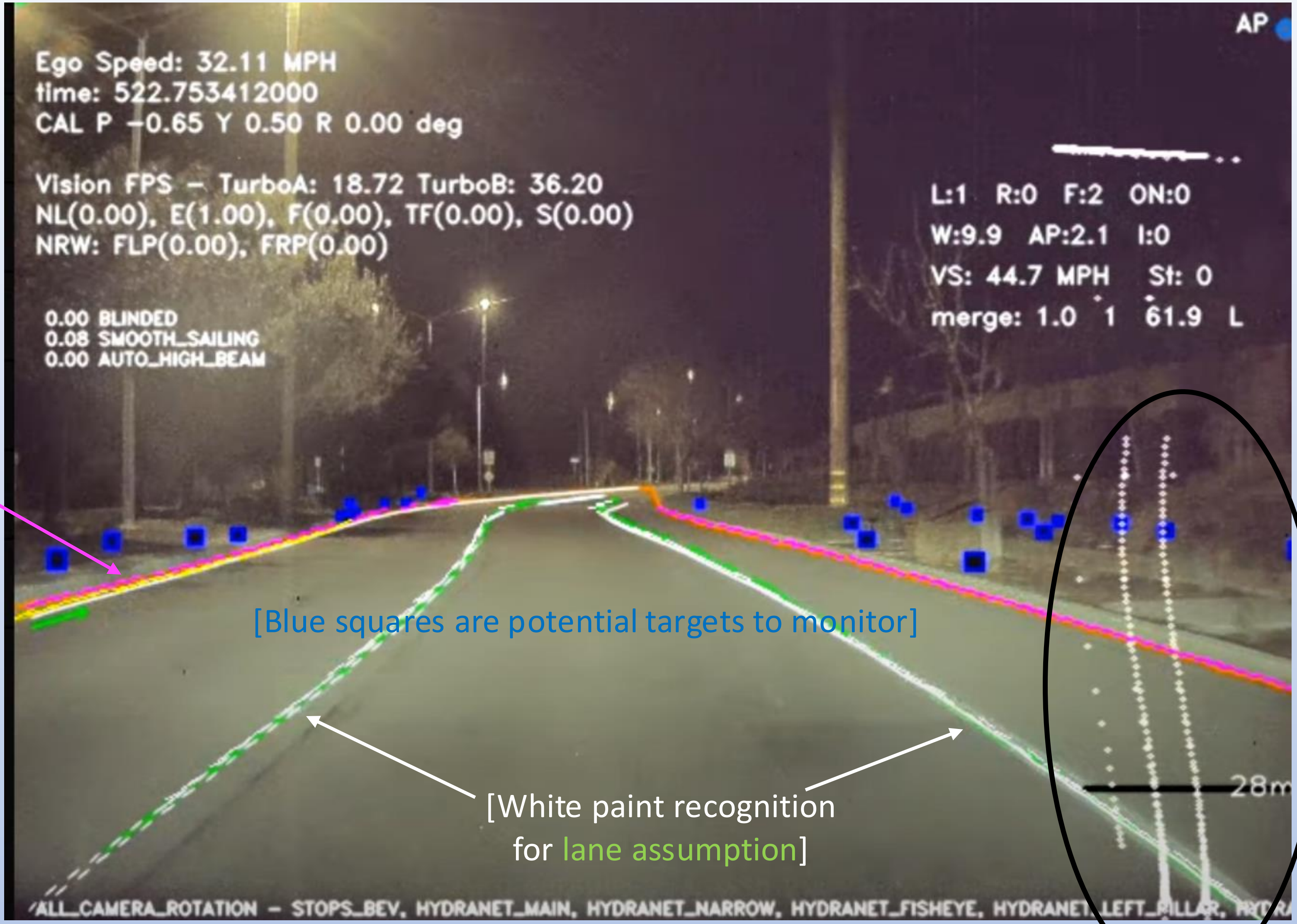
2 serious crashes

18 contact events

0 injuries

Tesla Integrated Sensor System – Simple background

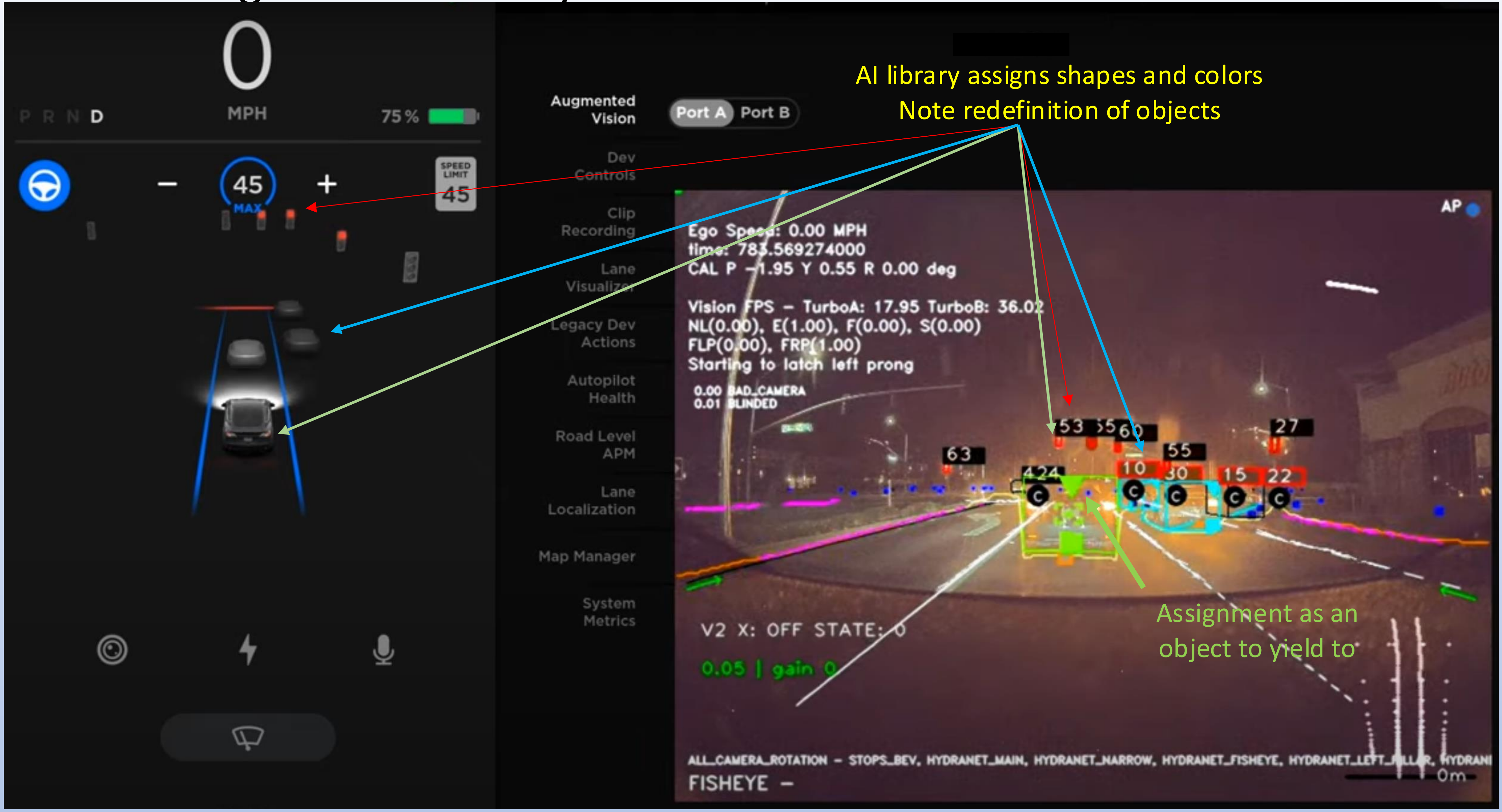
Curbs assigned a location and profile



Map view created for what is visible

Map created is continuously compared to GPS map

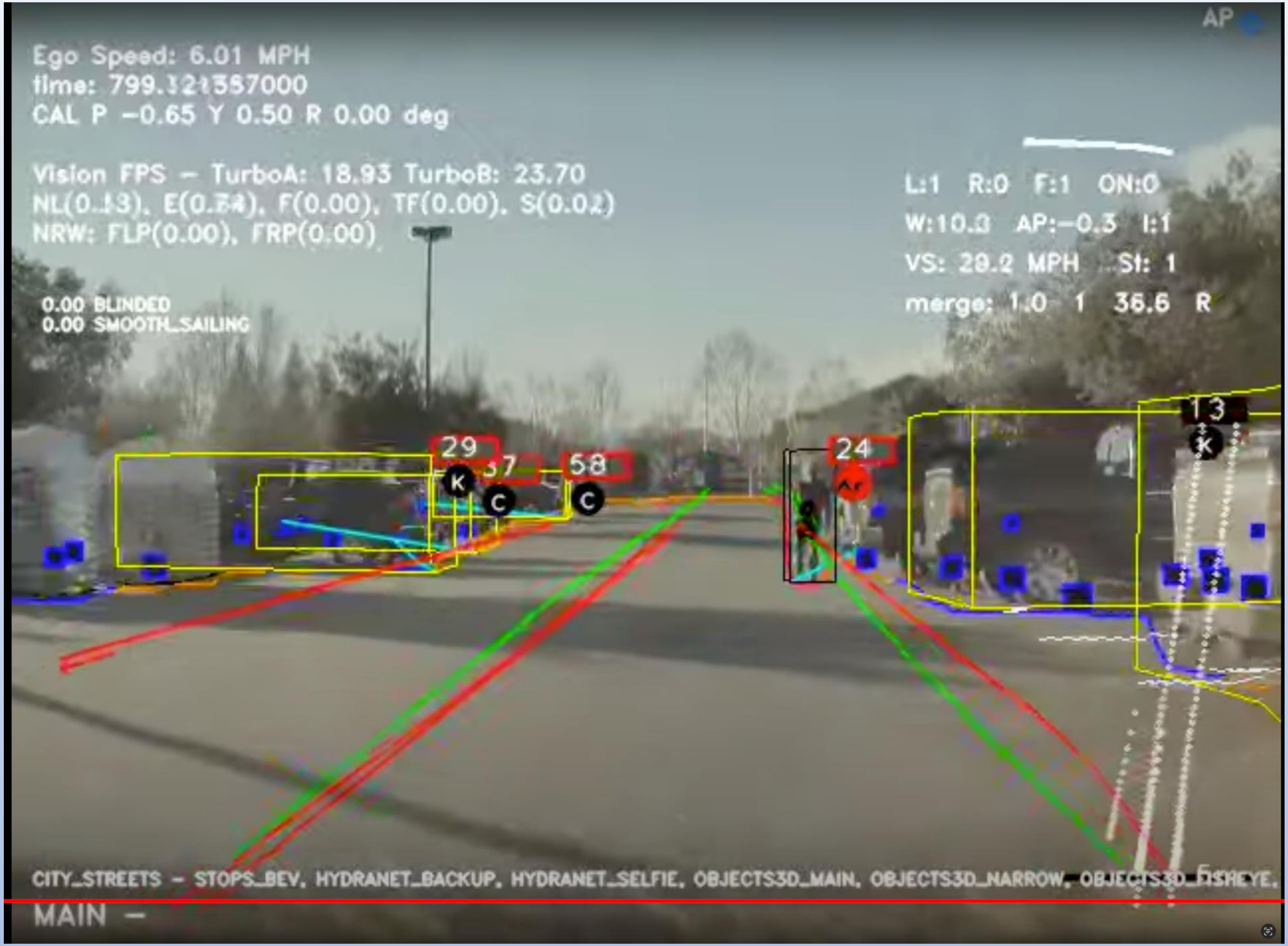
Tesla Integrated Sensor System – Urban Environment



HowItBroke.com

Tesla Integrated Sensor System

Congested area assignment of shapes to vehicles and pedestrian

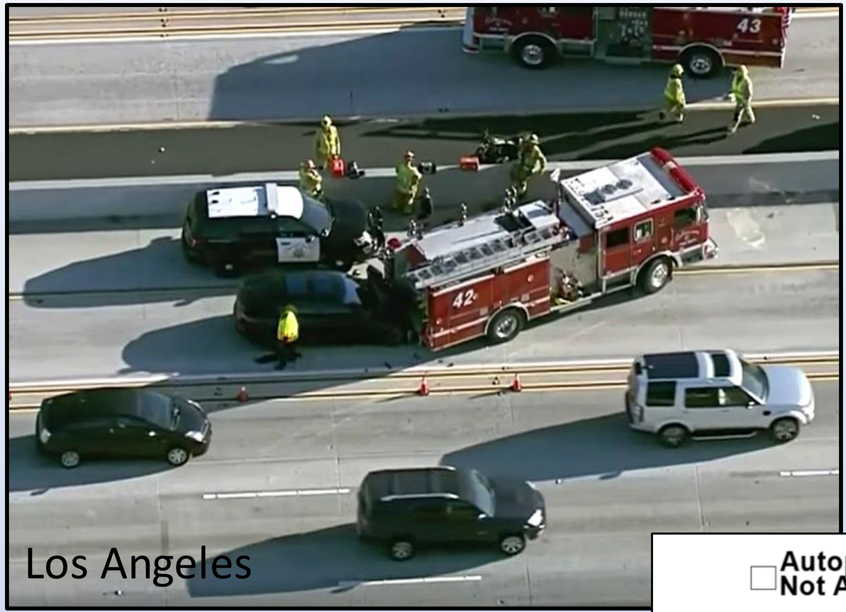


HowItBroke.com

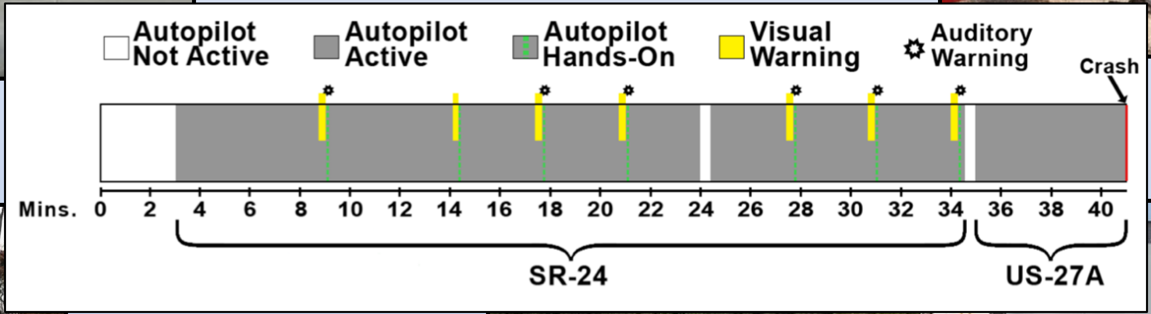
Model S Drove Beneath Trailer - Why?

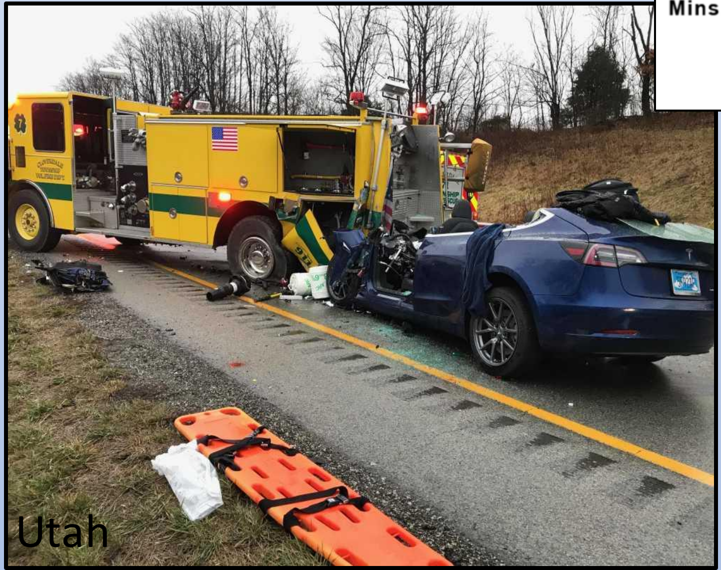
Williston FL, May 7, 2016, 4:36pm, NTSB/HAR-17/02

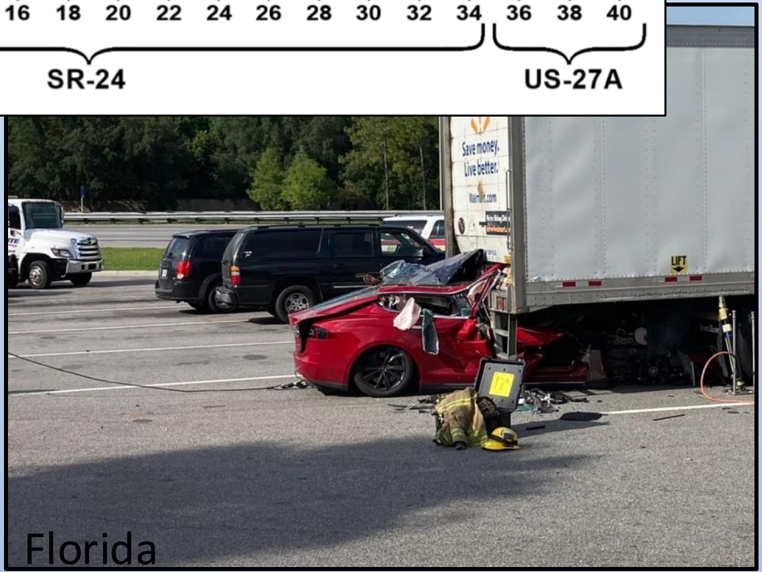
Common Theme in ADAS Equipped Vehicle Accidents


Los Angeles

Issue #1
Driver "Pavlov's Dog" Response




Utah

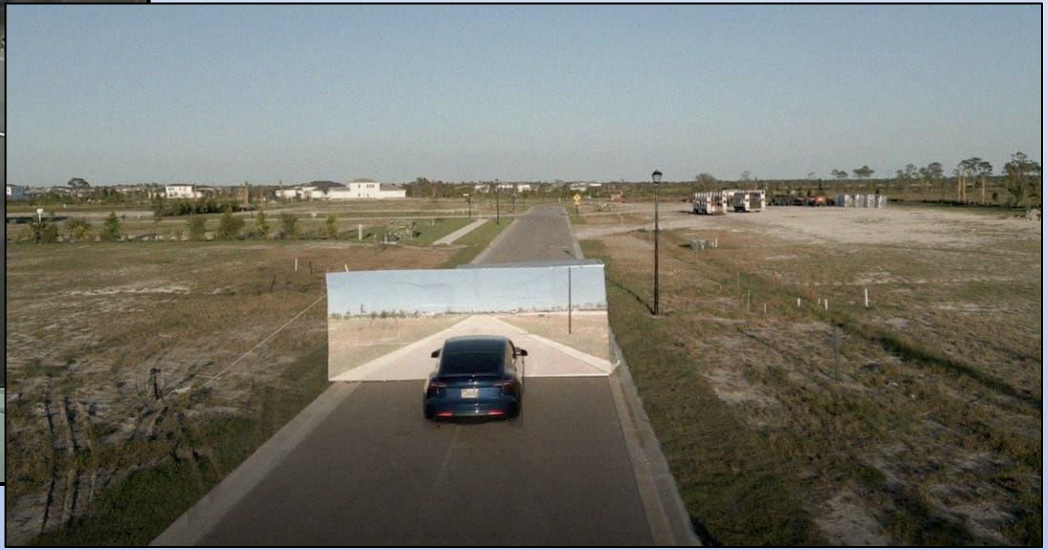


Florida

HowItBroke.com

Issue #2: Cameras assigning block shapes have difficulty in differentiating stationary items high enough to pass under

Vehicle will drive through photo

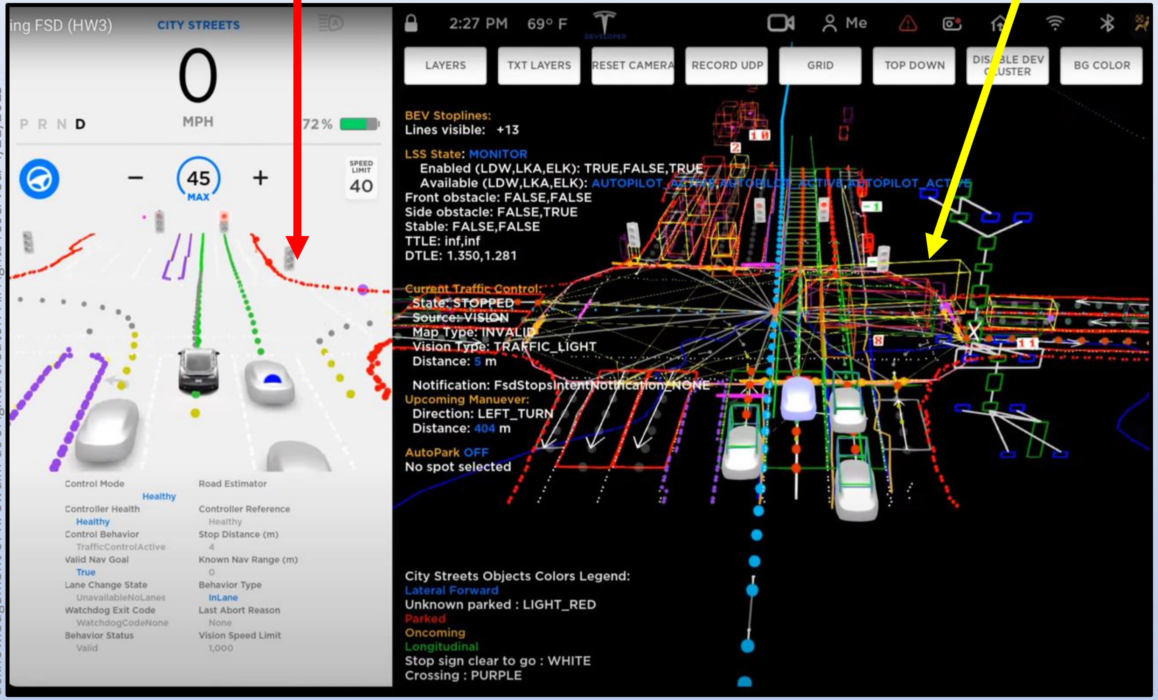


Example: Recognition of Crossing Truck at Intersection (Car Stopped)

Is it a truck three feet above the road?
An overpass?
A sign to drive under?

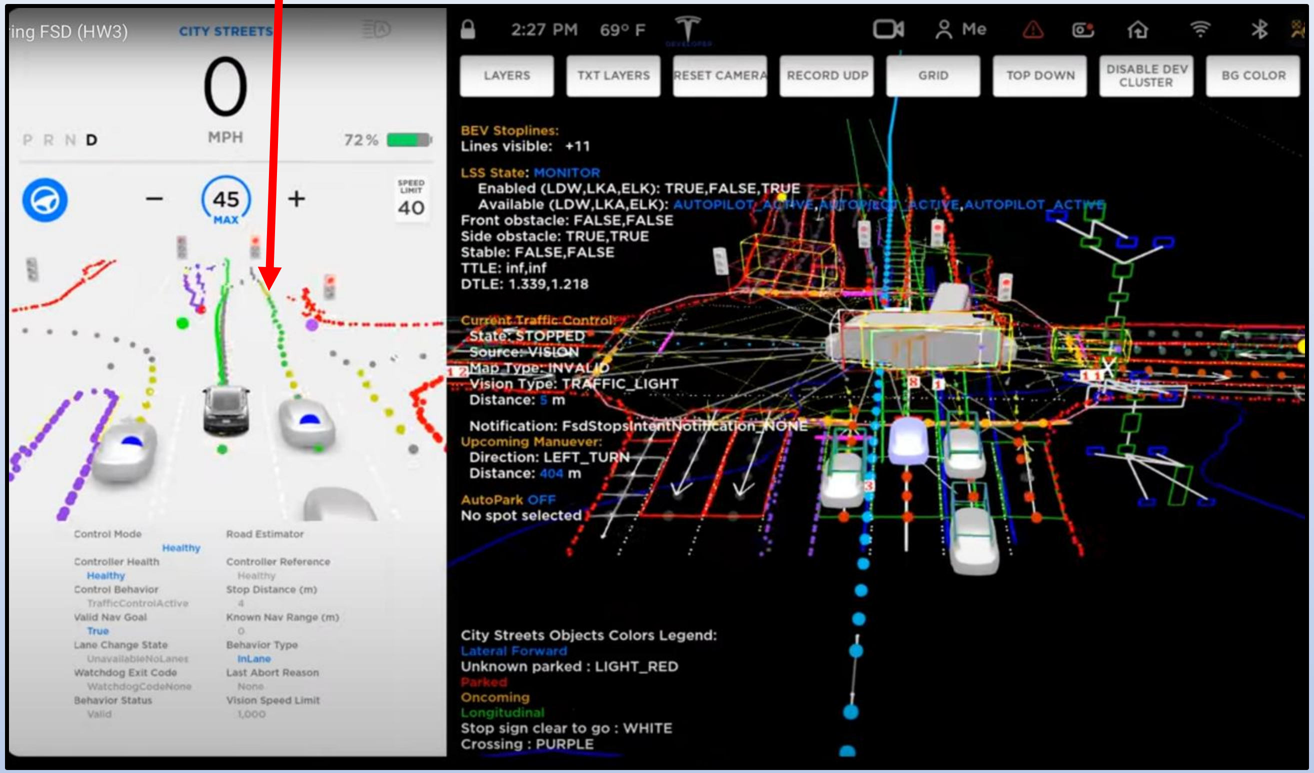
No truck

Yellow block for potential truck



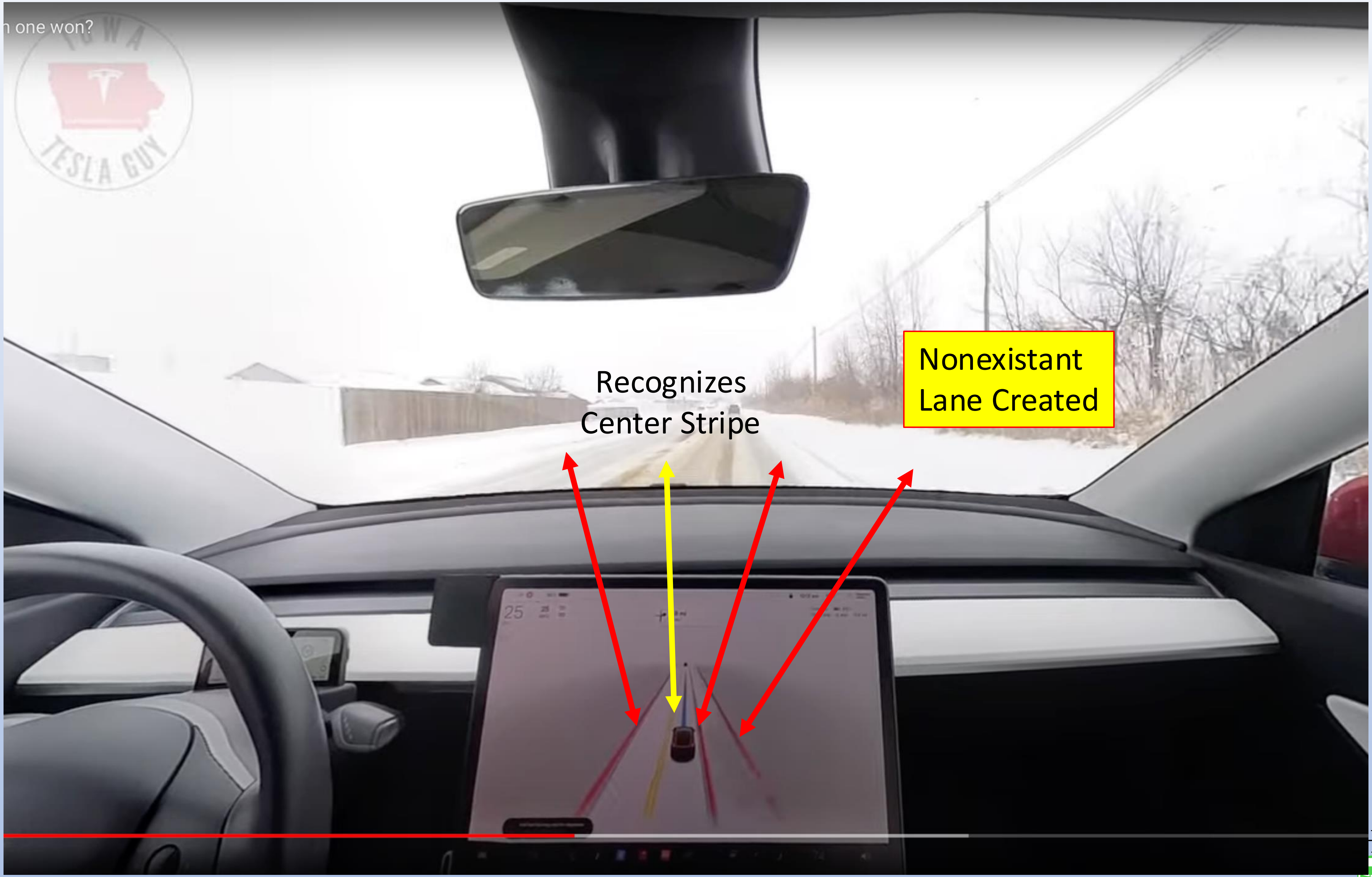
Still no truck

Assignment then indecision
(Cab at both ends)



HowItBroke.com

Weather and Road Conditions Can Degrade Sensors



Spoofing Automated Vehicles

Chosen Pattern Injection

Makes vehicles detect items which do not exist

Example: Signs printed on T-shirts

Driving Aggressively

Makes vehicle yield

Altered speed signs

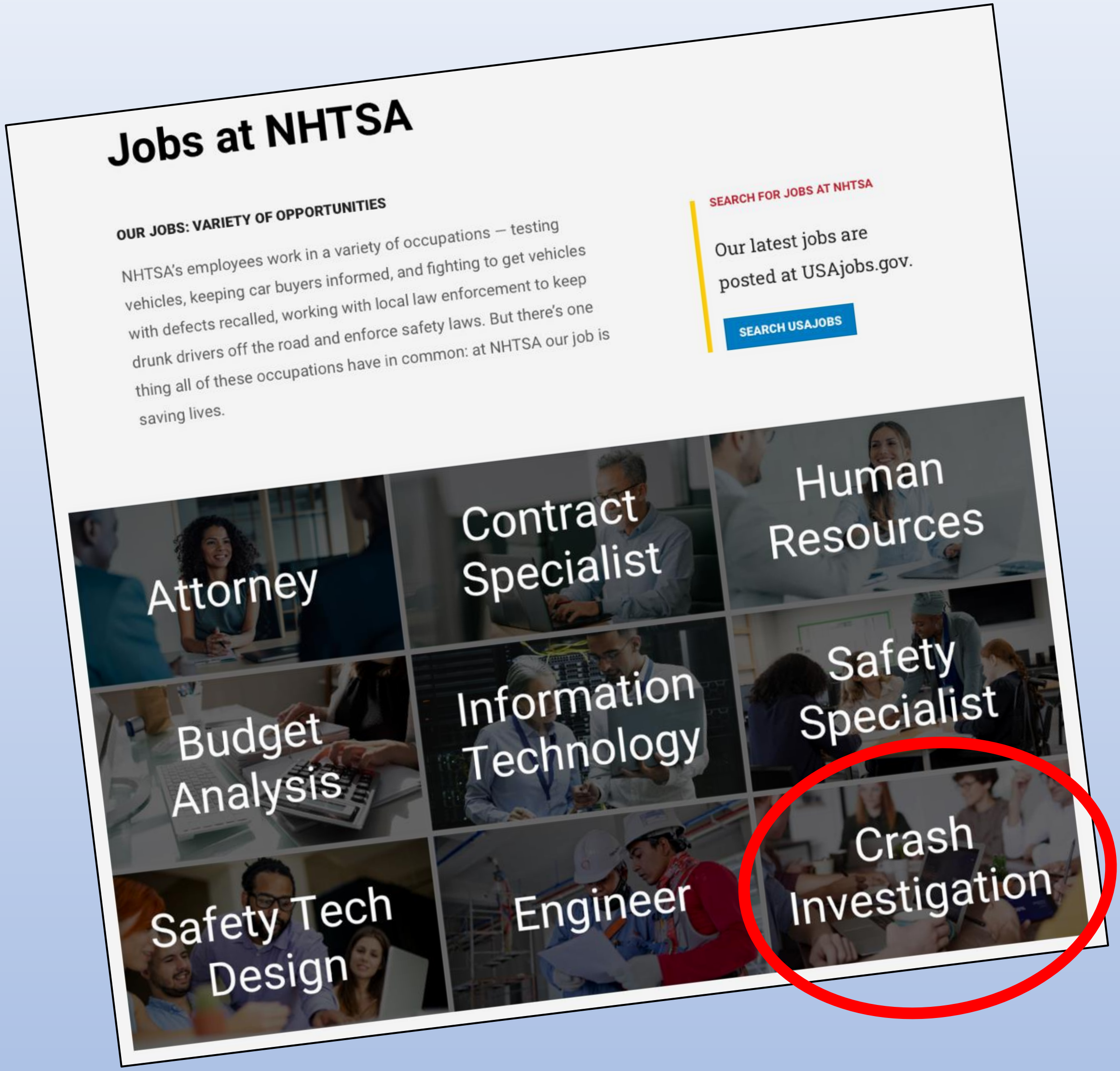
Temporary Physical Items

People surround vehicle

Cover sensor with aluminum foil

Cones

Now that you are experts
CONGRATS ON YOUR NEW JOB!!!

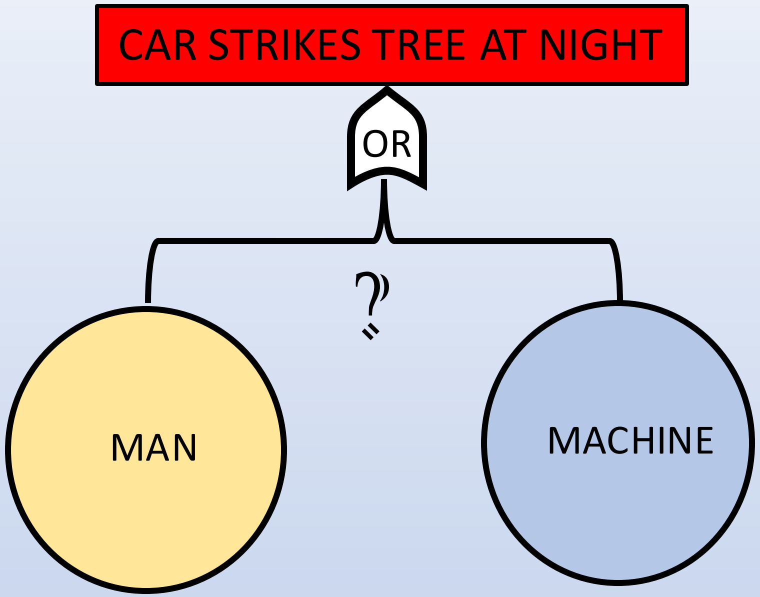


As part of Office of Defect Investigations (ODI)

You are part of a team investigating accidents involving ADAS.

Question - Should ADAS be banned?

ADAS Accident Investigation in College Park, MD



Failure Logic Tree

CAR STRIKES TREE AT NIGHT

Collect basic facts for each of the
5 Ms & E:

MAN

METHOD

MACHINE

MATERIAL

MEASUREMENT

ENVIRONMENT

Interview Notes of driver (Man)

Daisy DooRite, age 21,
123 Snobbish Court, College Park, MD,
Tel 301-XXX-YYYY

- Time of accident about 1 am.
- Was coming back to school from home in New Haven, CT after early dinner with parents.
- Boring drive due to lots of weekend traffic and sat on I-95 for periods of time.
- Ran out of drinks and wanted one to stay awake. Was waiting to arrive to use toilet.
- Near school was driving through the woods because I-95 was still so backed up. The road is dark but is a good back route.
- At time of accident the car was on autopilot and driver had hand on bottom of steering wheel. It never disengaged.
- The car just decided to turn the wrong way.
- Couldn't use the car phone because she had her boy friend's and it wouldn't hook up to the car. Did have charge cable.
- Driver slammed on the brakes but car wouldn't stop and the steering wheel was torn out of drivers' hands.
- No injuries. Intends to hire lawyer to sue car manufacturer.
- [*Police on scene reported no evidence of alcohol or drug impairment. Tesla call center reported collision at 2:21am*]

Vehicle at tow lot

Tree struck in curve

Start of 48 Hour Driver History (Man)

Date	Time	Item	Source
X/13/202X		[Fill in for previous day]	
X/13/202X	20:30	At house of friend	Driver interview
X/14/202X	00:30	Went to bed	Driver interview
X/14/202X	02:30	End of texting	Phone records
X/14/202X	07:00	Awoke to shop with Mother	Mother interview
X/14/202X	17:00	Departed parents house	Driver interview
X/14/202X	17:10	Receipt for Coca Cola and pretzels	Receipt found in vehicle
X/14/202X	19:30 [est]	Toilet stop	Driver interview
X/14/202X	22:00 [est]	Toilet stop	Driver interview
X/15/202X	02:21	Accident	Vehicle data

Actual rest started

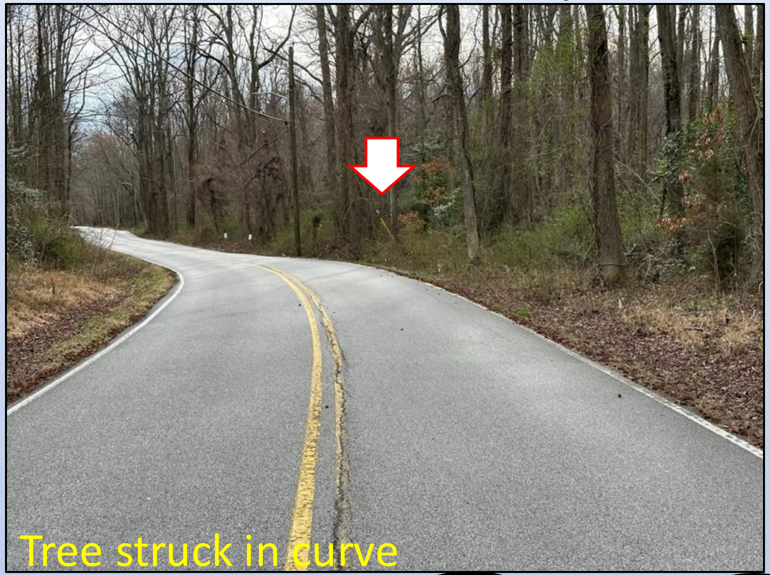
4.5 Hours sleep

9:21 Underway
19:21 Hours awake

Failure Logic Tree – What do you notice at scene? (Environment)

SCENE:

- Dark location with no street lights. Posted 35 mph
- Dry pavement with no skid marks observed
- Straight wheel marks through dirt to tree
- Pavement markings worn and road edge partially obscured with leaves
- Passed a house security camera showing speed of 40 mph



Tree struck in curve

No braking skid marks

Worn pavement

Optical sensor tolerances

Dark

5 Ms & E:

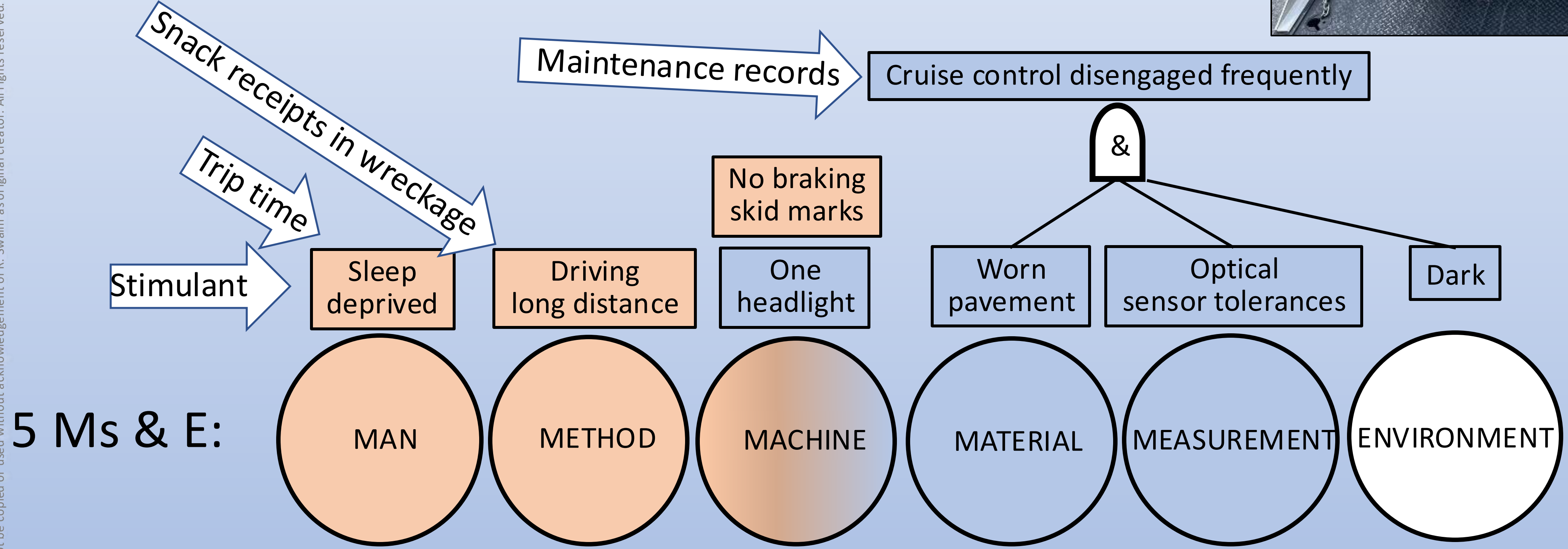
MAN | METHOD | MACHINE | MATERIAL | MEASUREMENT | ENVIRONMENT

HowItBroke.com

Failure Logic Tree – Vehicle (Machine)

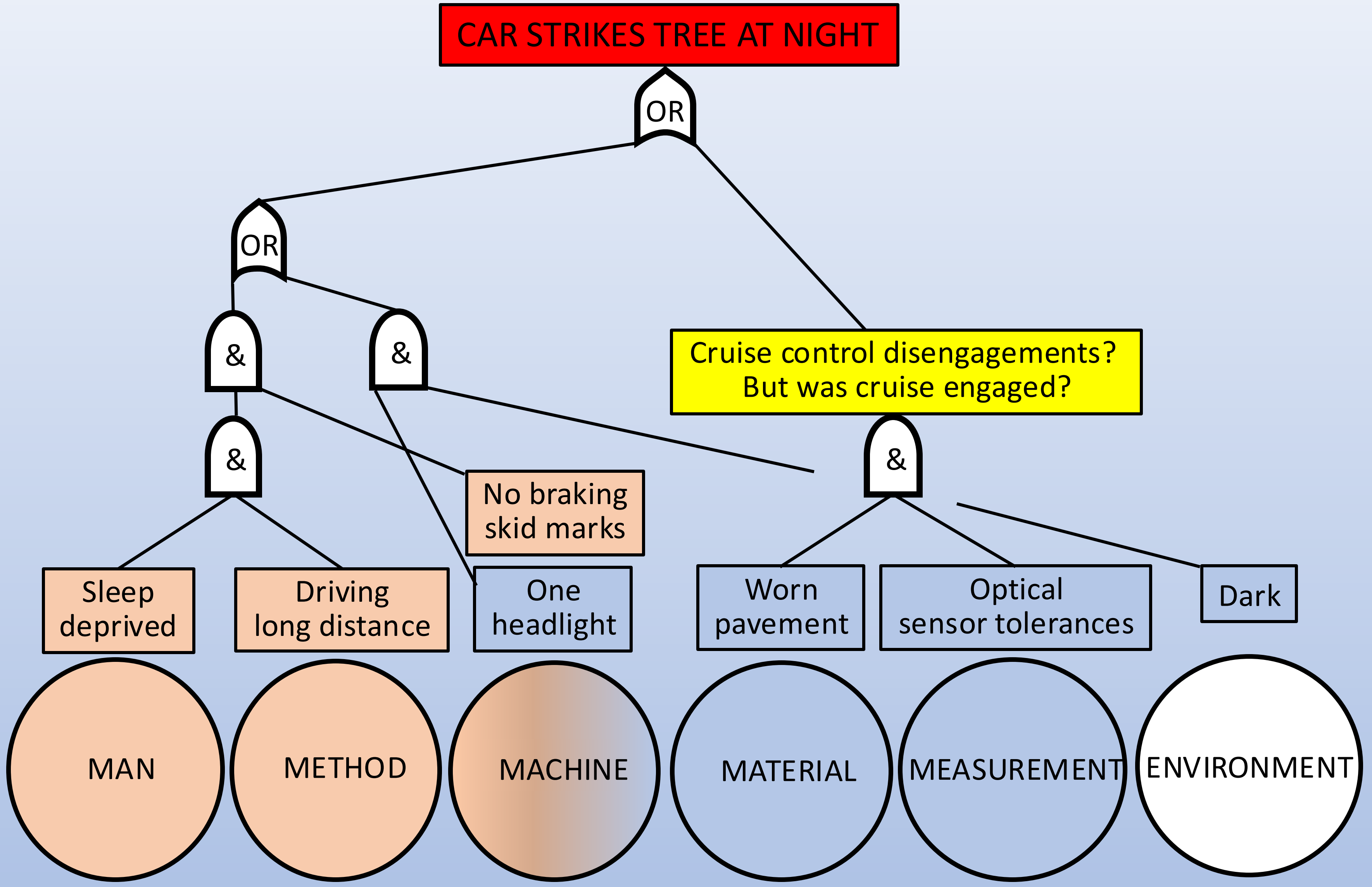
VEHICLE FINDINGS:

- Time on receipt for pretzels and Cokes from store in Connecticut
  - Long trip time [*9 hours to 2:21 am*]
  - Long driving distance [*300 miles*]
  - Six empty Coca Cola cans [*Effects of stimulant wearing off*]
- One headlight tested inoperative after accident
- Dirty windshield ahead of driver mirror [*Contains triple camera lens*]
- Glovebox service receipts state cruise control disengages periodically



Failure Logic Tree – Combined Man and Machine Facts

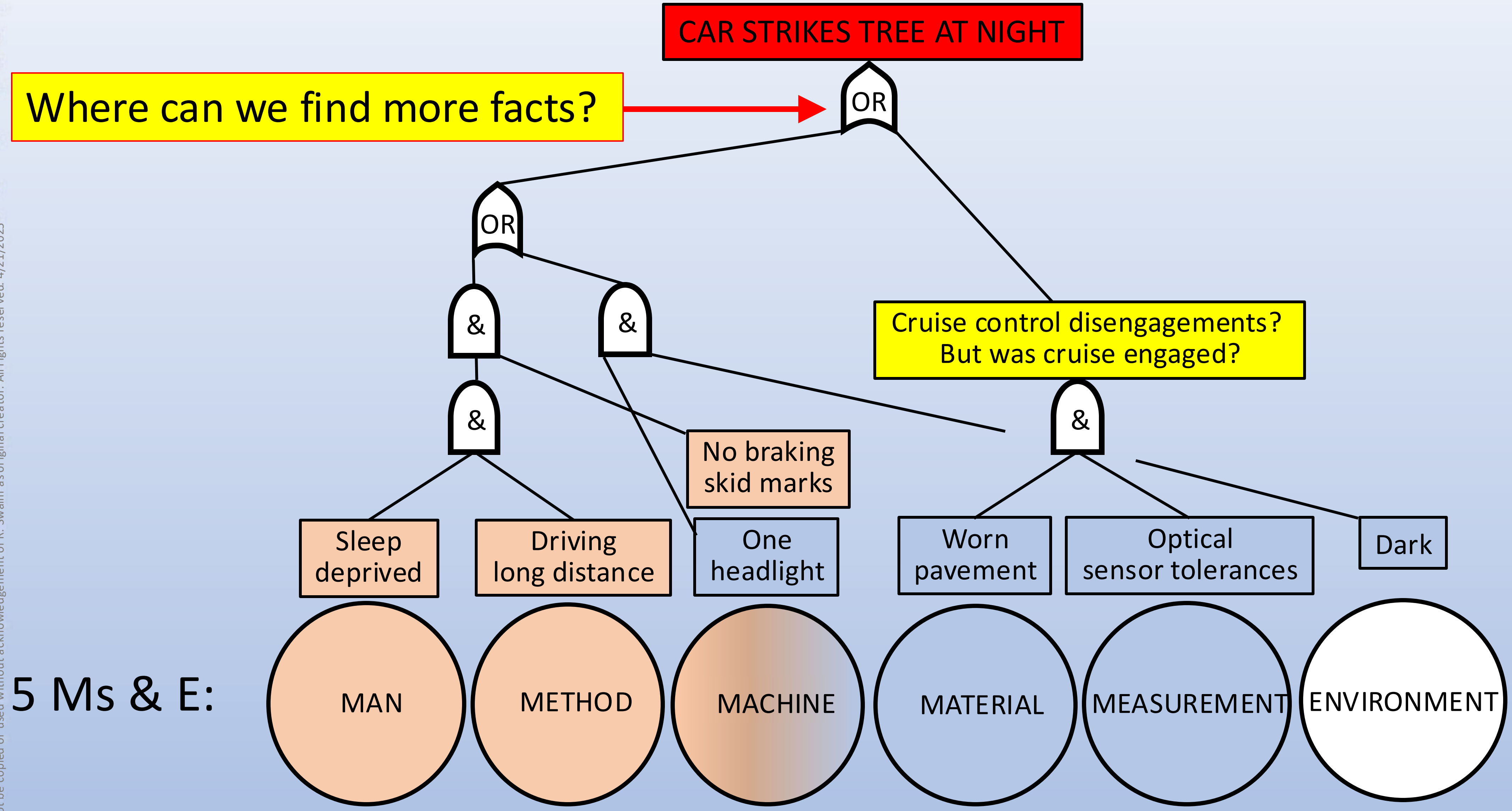
Now it could be the driver OR the car



5 Ms & E:

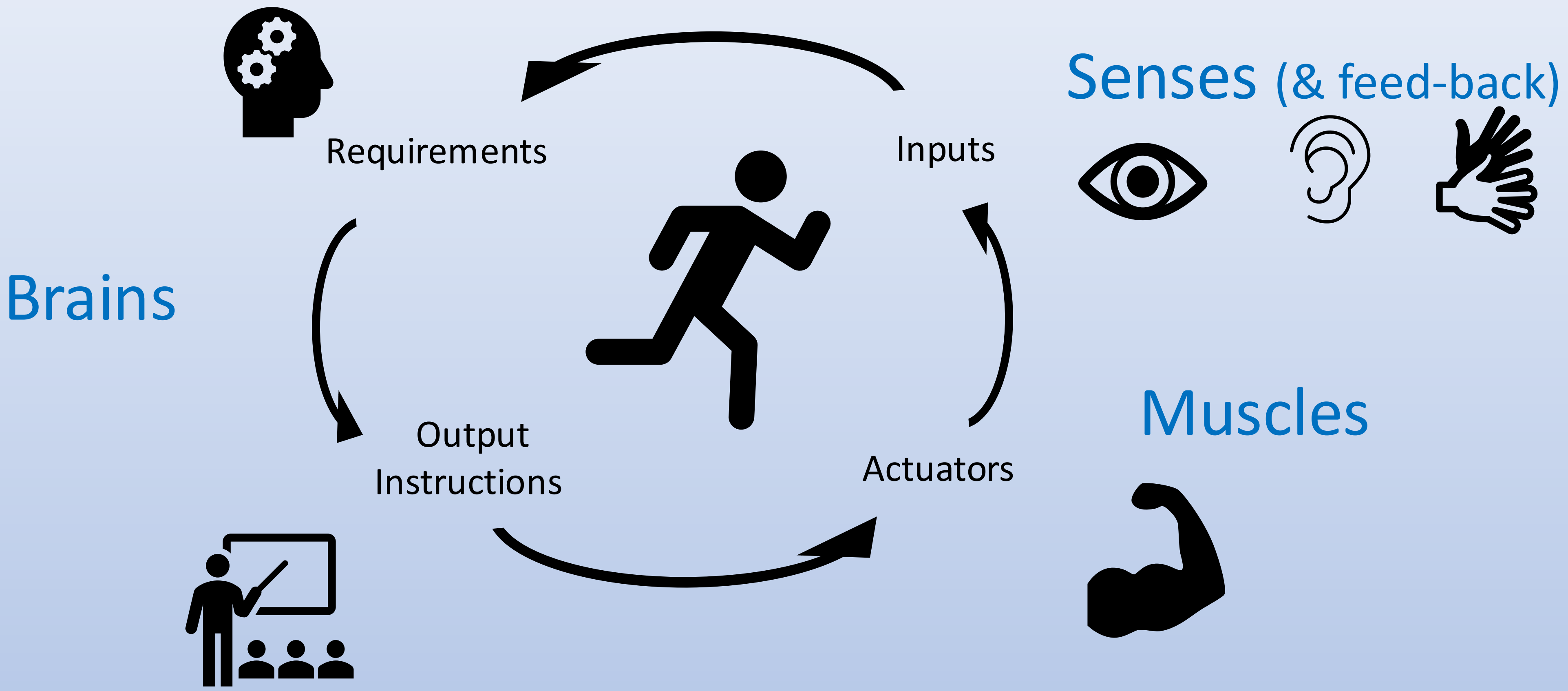
Failure Logic Tree – Combined Man and Machine Facts

Now it could be the driver OR the car



Machine - Continuous Loop of Automated Systems

Brain functions consider and create output instructions
For muscles to implement
Followed by senses reporting status of the movement back to the brain



Continuous Loop of Automation is Similar to Anatomy

Brains

Design assumptions

Potential software **conflicts**

Databases & lookup tables

Calculate position

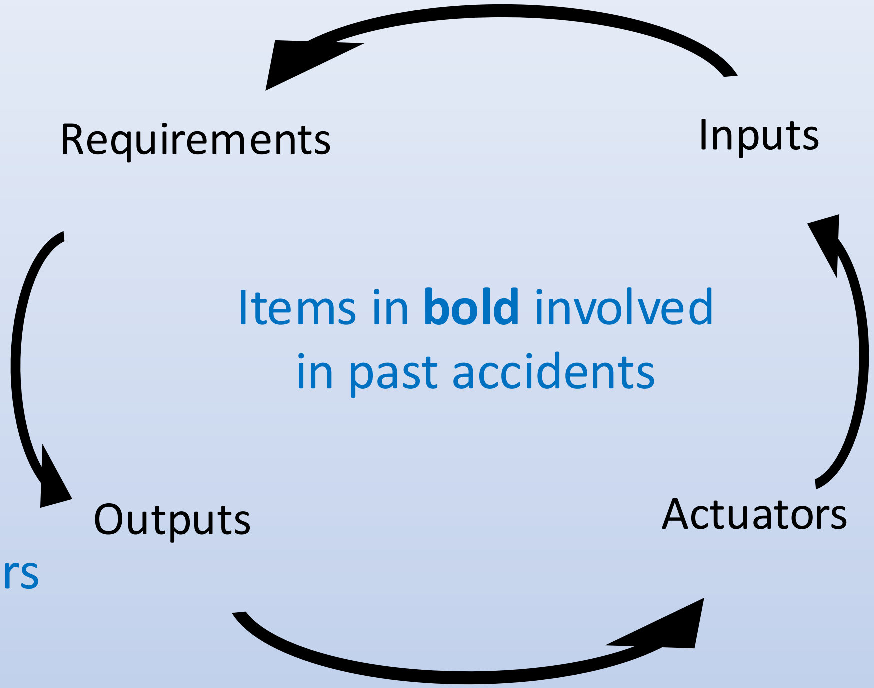
Compute delta to requirement

Buffers, timers, and filters

Compute needed corrections

Guidance commands to actuators

Displays to humans



Senses (& feed-back)

Driver mechanical & **switches**

GPS & other **NAV**

Camera and **optical sensors**

RADAR, LIDAR, & **RF based**

Environmental sensors

Feedback of device positions

Muscles

Mechanical

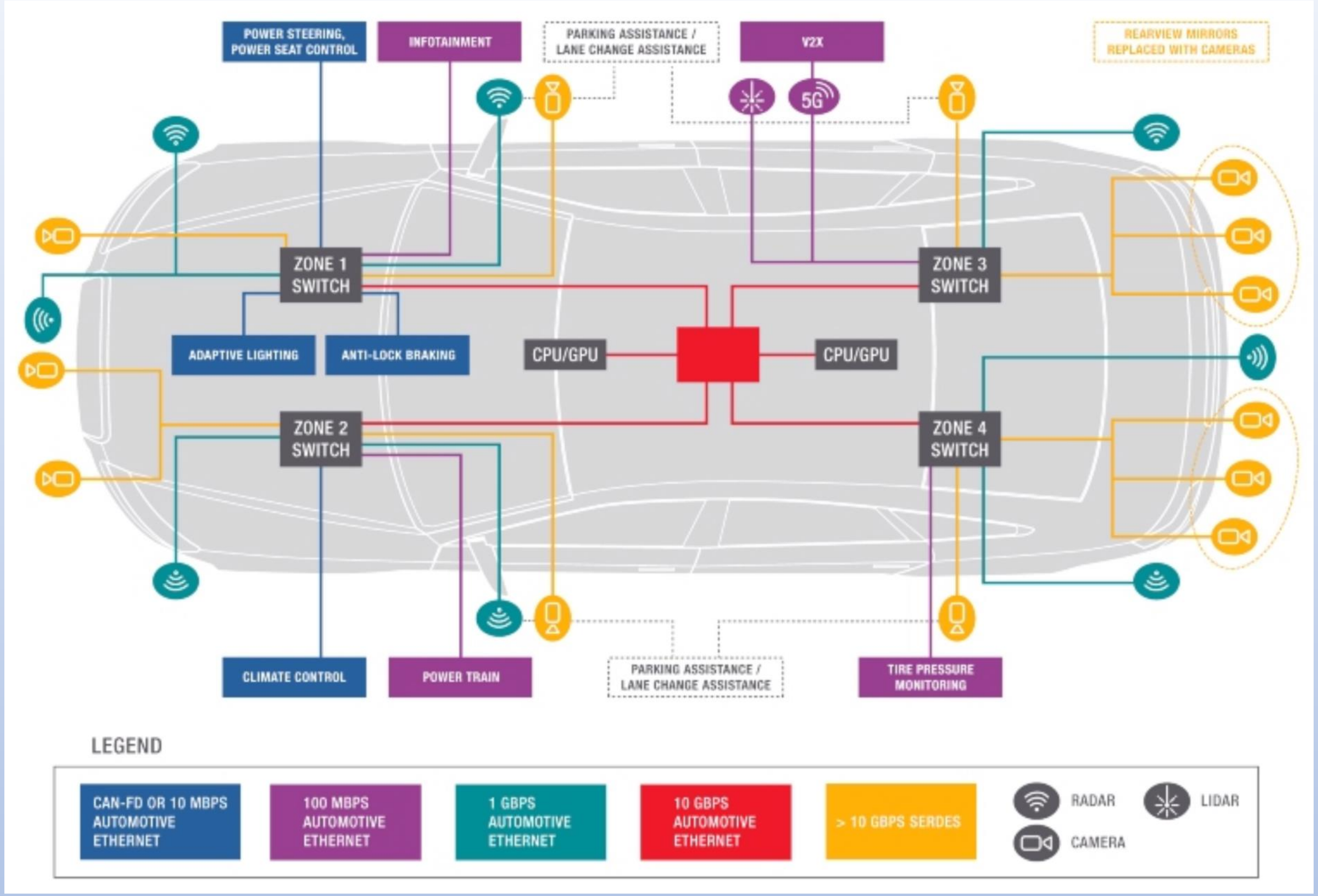
Electric

Hydraulic

Need more data!

Data?

Most of these are recorded



Vehicle Data Recorders

Information Access Depends on Type of Investigation

Criminal – Government may not release ANY data

Safety – Government may release partial data, typically not video or audio

Civil – Typically requires court subpoena. May be denied.

Technical – May or may not get access

Data and Recordings

Frequently embedded in multiple devices for various types of information

Vehicle devices typically not hardened like aviation "Black Boxes

May contain dozens to thousands of parameters such as:

- Speed, Lat/Long (GPS), seat belt use, airbag deployment, impact sensor states, fault logging (OBD), automation engagement and level, cell temps and detailed EV battery data, motor temp, transmission status, ABS, ESC, throttle position, atmospheric pressure, OAT, headlight use, wiper use, door alerts, etc,

Parameter recording rates differ

- Example: Seatbelt status upon change of state vs vehicle speed at least once/second

Data Sources

Restraint Control Module (RCM)

Five Seconds of RCM Data

HWY18FH011, Mountain View CA, 3/23/2018

TESLA

Event Data (Event 1)

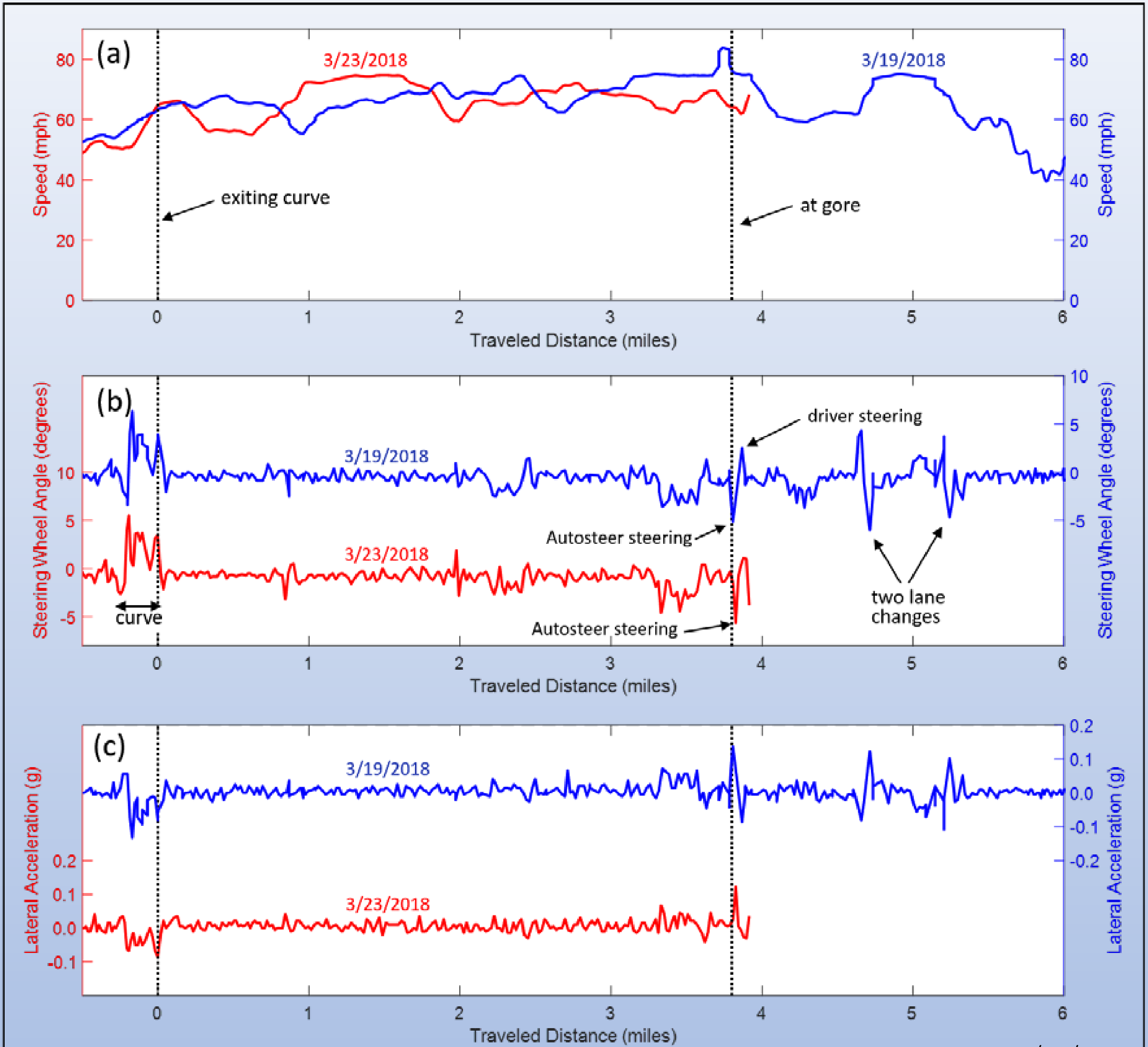
Time (sec)	Vehicle Speed (km/h)	Accelerator Pedal (%)	Rear Motor Speed (rpm)	Service Brake	Stability Control	ABS Activity
-5.0	102	0	6799	Off	On	Off
-4.5	101	0	6713	Off	On	Off
-4.0	100	0	6641	Off	On	Off
-3.5	100	0	6612	Off	On	Off
-3.0	100	0	6689	Off	On	Off
-2.5	101	0	6766	Off	On	Off
-2.0	104	0	6937	Off	On	Off
-1.5	107	0	7104	Off	On	Off
-1.0	109	0	7284	Off	On	Off
-0.5	112	0	7433	Off	On	Off
0.0	114	0	7584	Off	On	Off

Media Control Unit (MCU)

From Media Control Unit and Autopilot ECU:
Precise time, Speed, Steering wheel position, Accel pedal position, Driver brake pedal, A/P Status, Faults, Longitudinal and Lateral G forces, lead vehicle distance

HowItBroke.com

Example of Carlog Data Showing Driver Taking Control



HWY18FH011, Mountain View CA, 3/23/2018

Other Parameters Available Include:

Speed,
Lat/Long (GPS),
Sensor buffers for LIDAR/RADAR/etc
Seat belt use,
Airbag deployment,
Impact sensor states,
Fault logging (OBD),
Automation engagement and level,
Cell temps and detailed ev battery data,
Motor temp,
Transmission status,
ABS,
ESC,
Throttle position,
Atmospheric pressure,
OAT,
Headlight use,
Wiper use,
Door alerts,
Etc,

Recording devices to look for

ON VEHICLE (Some require continuous 12V source)

- Vehicle event recorder (Precise time of accident, speed, G forces, etc)
- Onboard video recorder
- Motor controller memory,
- EV Battery Battery Management System (BMS)
- Anti-skid braking system memory (ABS)
- Other . . .

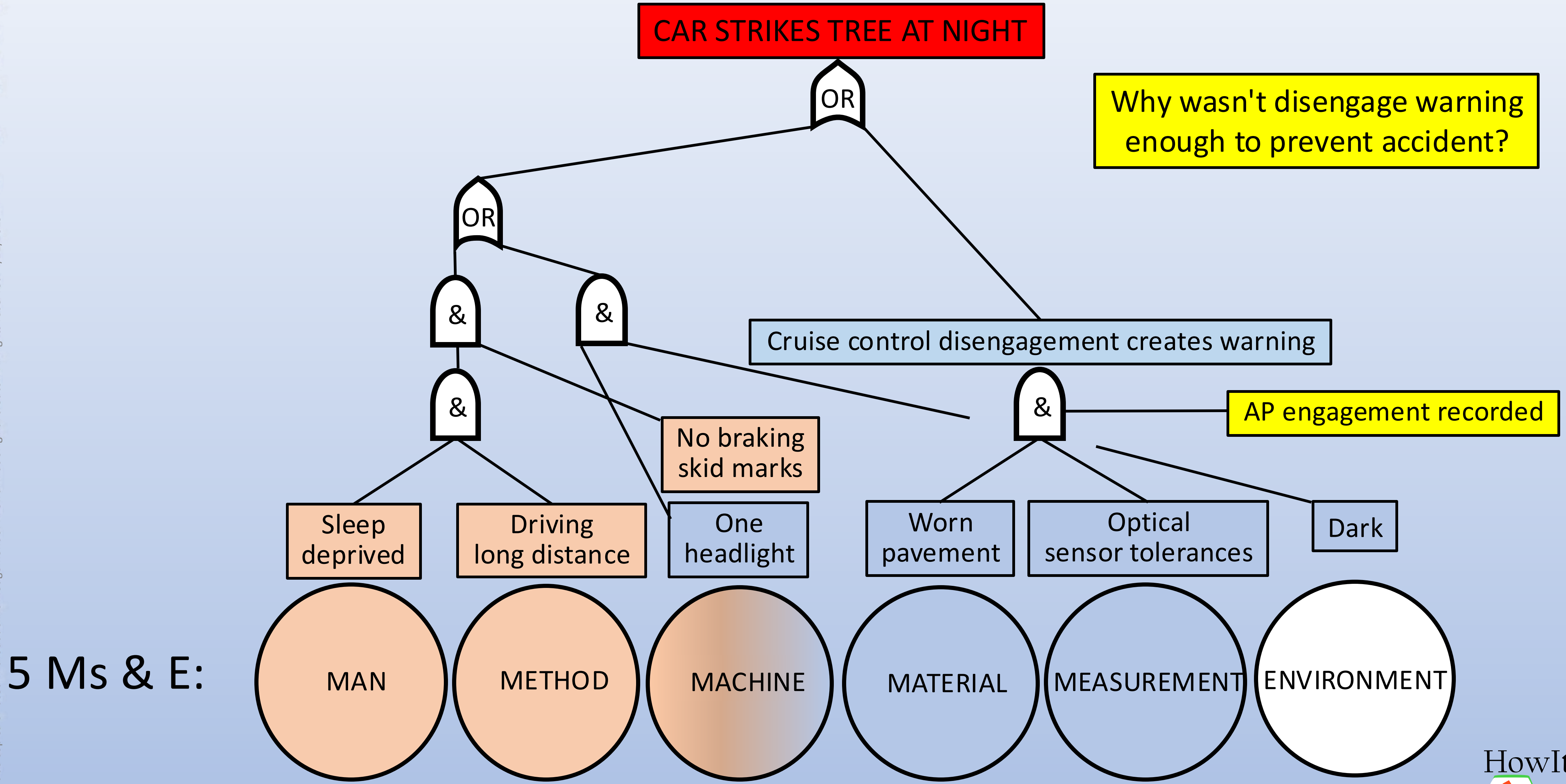
EXTERNAL

- Cell phone – phone, data, GPS, camera
- Roadway system - traffic video, timers, and other devices
- Stores and other business security cameras

DATA IS SELDOM COMPLETE.
For example the following items are frequently not all available at same time:

- Look up maps – Need constant update
- GPS
- Optical – Road markings, sign markings, surrounding structure, other objects
- LIDAR/RADAR/WAVE

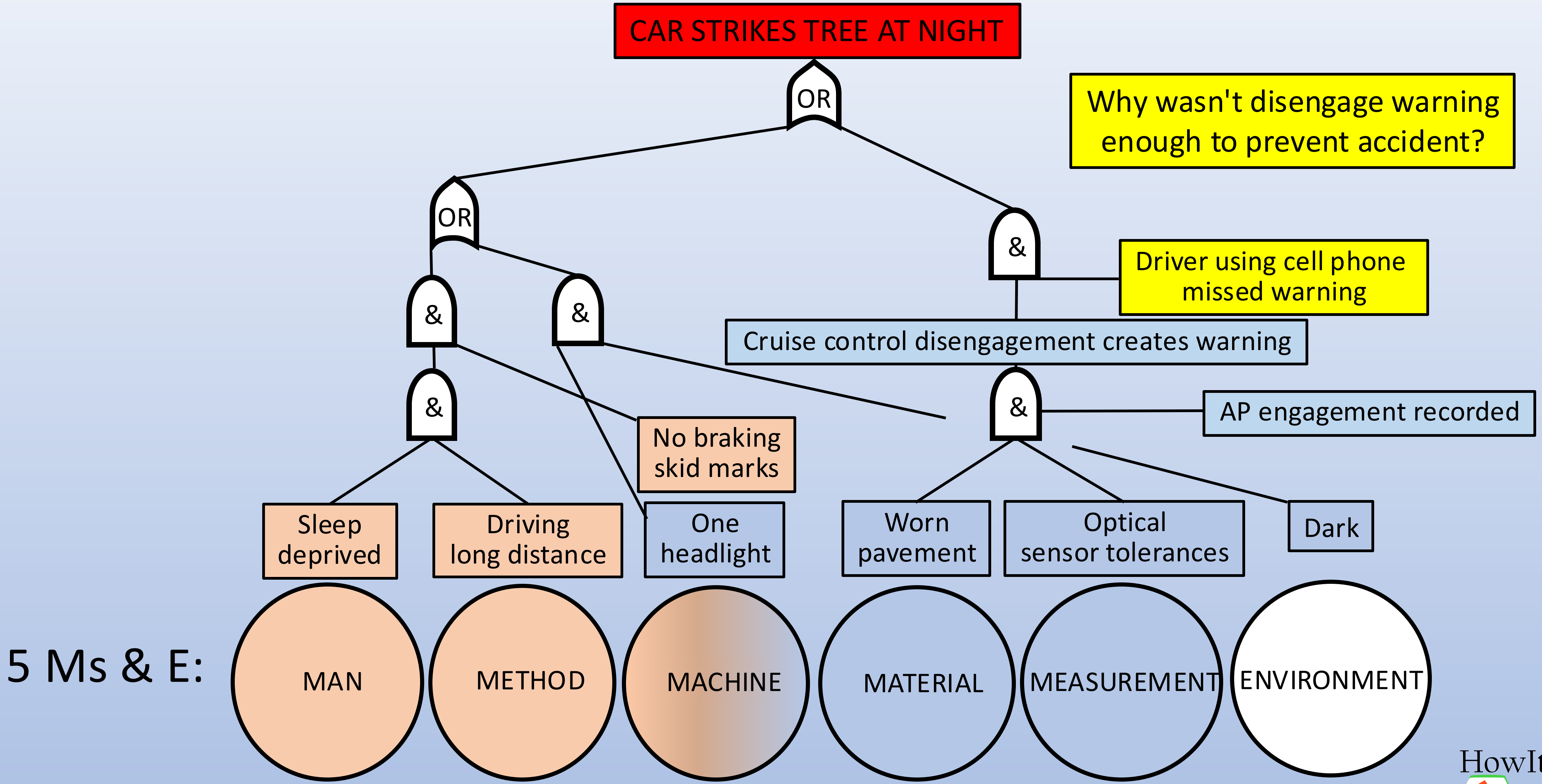
Failure Logic Tree – Remaining Question



Failure Logic Tree – Subpoena Phone Records

Driver iniated 11 separate calls during trip and received 5.

Most recent call initiated 7 minutes prior to accident time (2:21am).



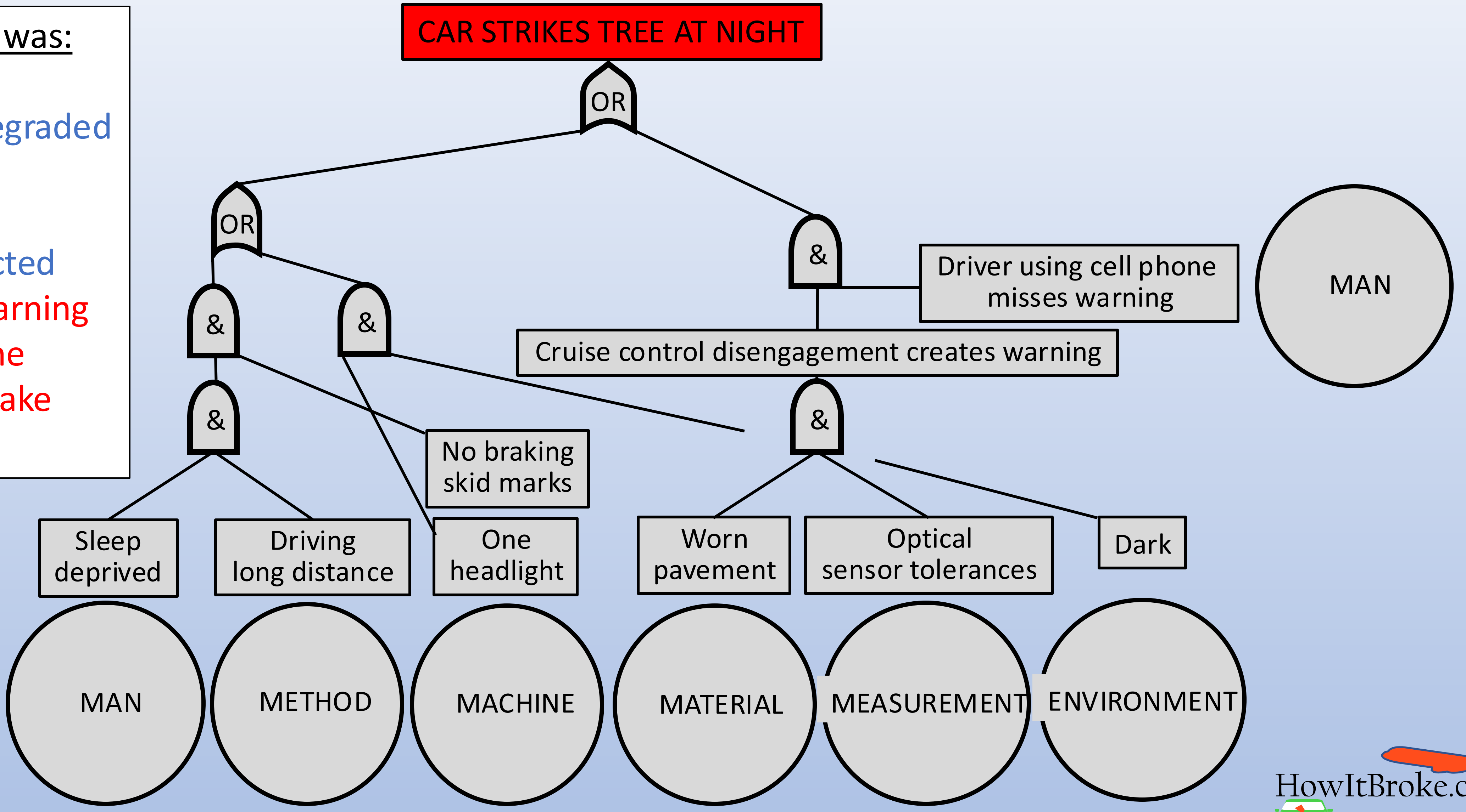
Failure Logic Tree – FACTS LEAD TO ANALYSIS / SEQUENCE

Now we find contributing factors included BOTH the driver AND the car

<u>Sequence found was:</u>

Tired driver
Cruise system degraded
    Pavement
    Optical system
Cruise disconnected
Driver missed warning
    Using cell phone
Driver did not brake
Car struck tree

5 Ms & E:



Chronology and Contributing Factors

As a result of the investigation and collection of all possible facts, a chronology for the accident was established which led to identification of the Contributing Factors:

Degraded / Fatigued driver: The accident time was at a low circadian rythym hour, driver cited sugar withdrawal symptoms, had driven a long distance, and been in vehicle for 9 hours.

The Cruise system operation was degraded due to:
- Worn pavement markings
- Optical system operation at the limits of design perception with the degraded pavement
- Dirt found over camera sensor array

The Cruise system disconnected.

The driver using the hands-on cell phone likely missed the warning that the automation system had disconnected.

The driver did not apply brakes on pavement.

The vehicle struck a tree.

Probable Cause

The Probable Cause for a case such as this example would likely identify the driver’s degraded responsiveness and distraction as the primary cause.

The failed headlight and degraded Level 2 automation might be considered as Contributing Factors.

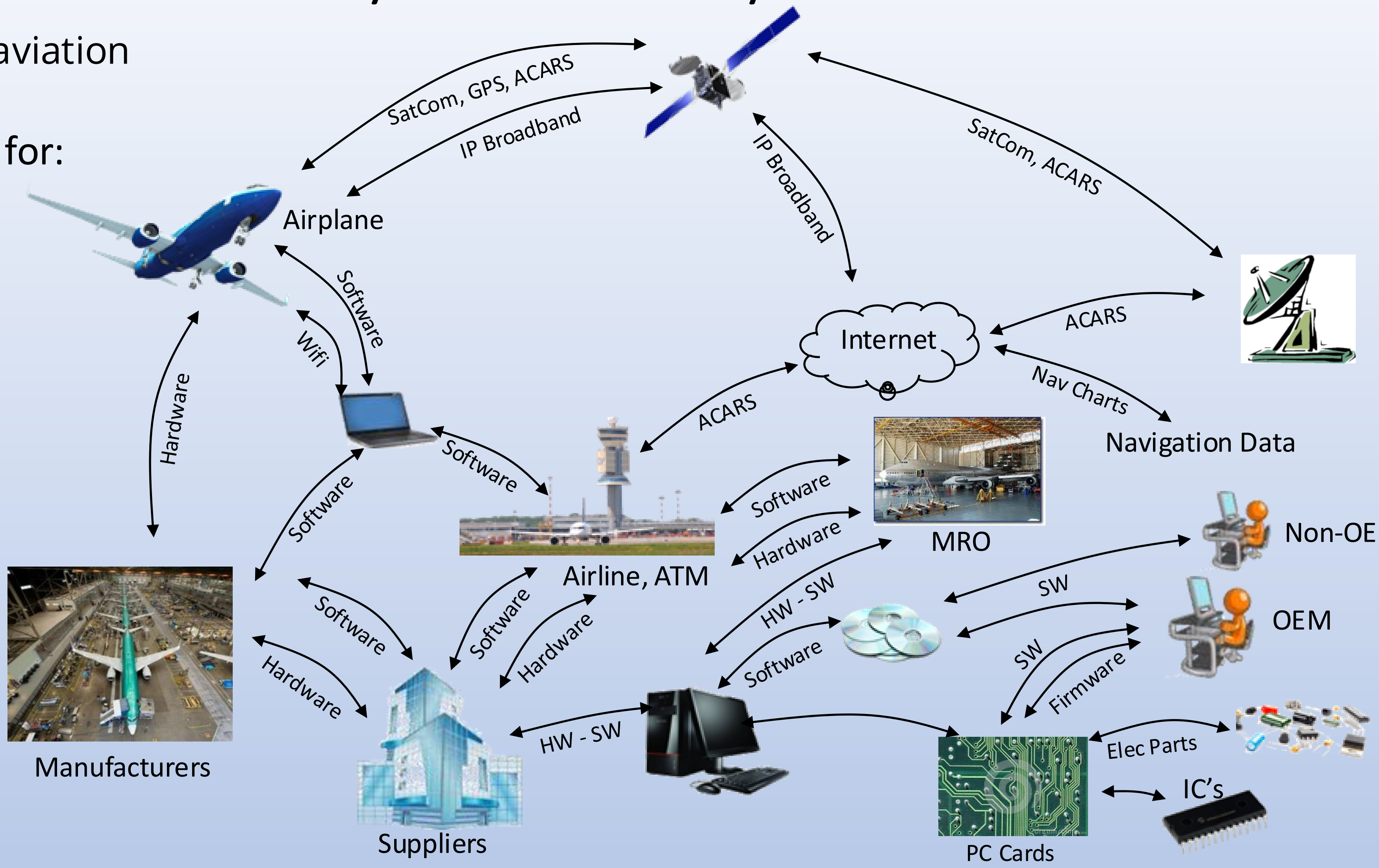
Numerous points create cybersecurity vulnerabilities

Attacks have taken place in aviation

Despite ISO 26262*, monitor for:

Intentional
- Database corruption
- Vehicle antenna inputs
- Sensor entries
- Software attacks

Unintentional
- EMI/HIRF environment
- Software conflicts
- Sensor conflicts



Adapted from Boeing Aviation Cybersecurity Diagram

Cybersecurity/hacking violations are a <u>crime</u> and <u>require</u> notification of law enforcement!

* ISO 26262 - Road Vehicles Functional Safety Package

HowItBroke.com

A Lesson From Aviation In Closing

Kettering Bug cruise missile 1918

Lawrence Sperry patented first autopilot in 1912
Triple redundant systems in airlines today - yet ...

...loss of control found in 43% of 2010-2014 fatal commercial accidents (37)

The #1 Autopilot related cause of accidents is human interface
Typically perception of autopilot performance was not what was expected

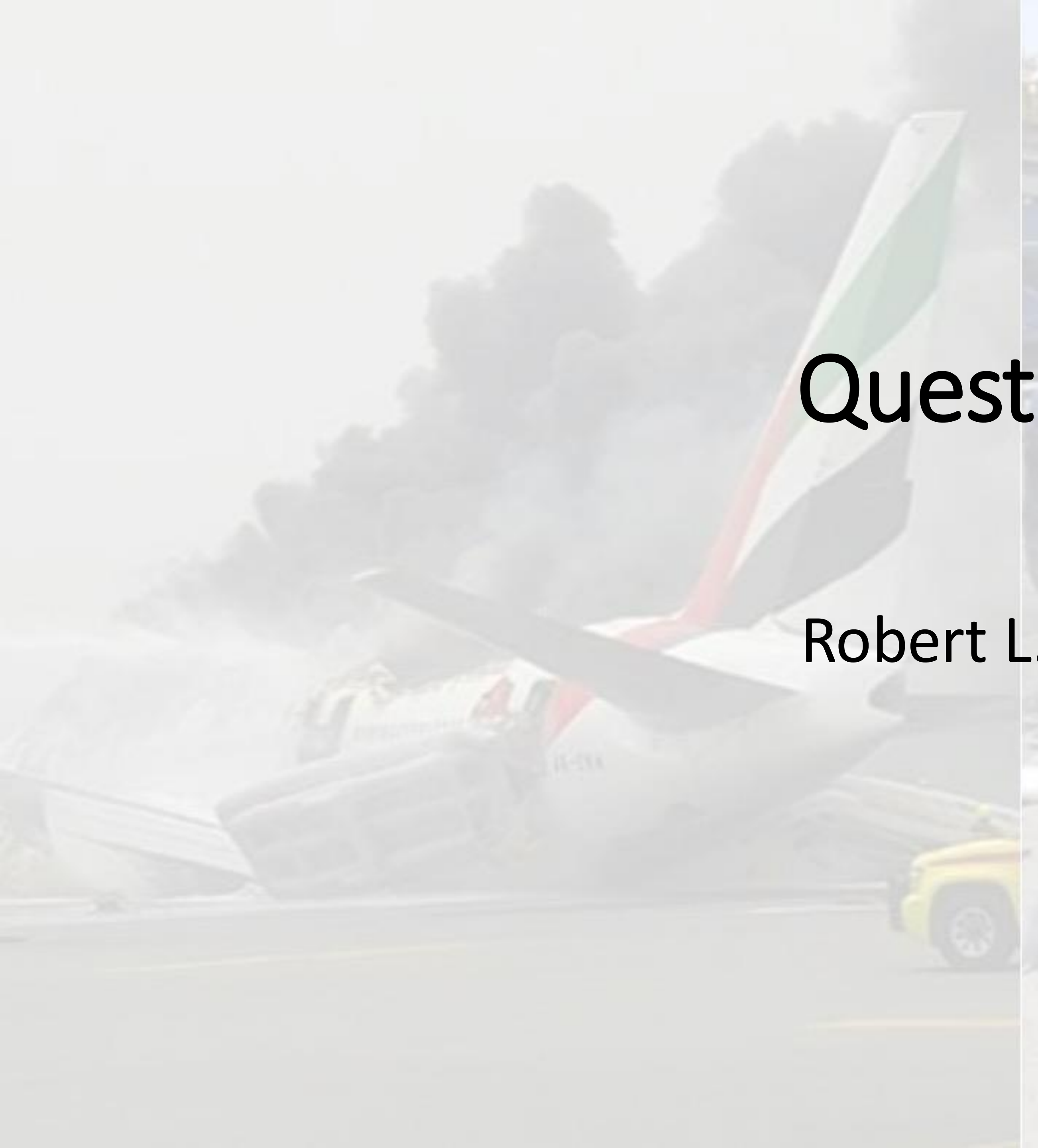
The #2 Cause was pilots disconnecting or getting "behind" the airplane

"What's it *[the autopilot]* doing now?"

Common airline crew saying on Cockpit Voice Recorder (CDR)

"Disappointment *[causing stress and errors]* is **the gap that exists between our expectation and reality"** – Maxwell

Examine to make sure that reality does not differ from expectations




Questions?

Robert L. Swaim

HowItBroke.com
Investigations
Engineering
Training