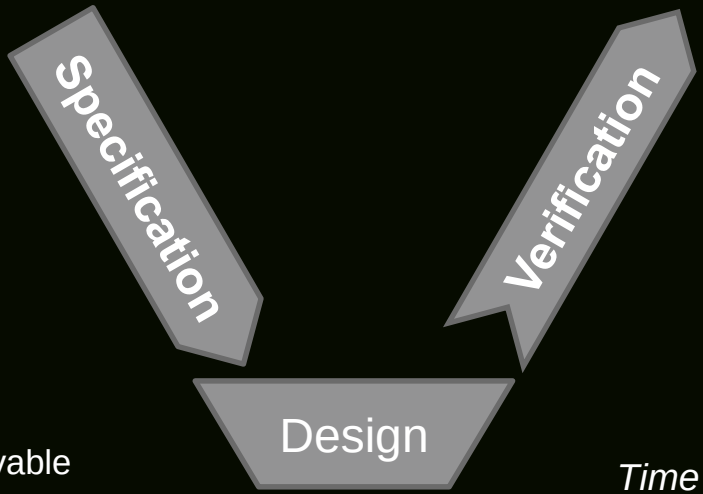
SAFETY FOR SELF-DRIVING VEHICLES

Dr. Jonas Nilsson
Dependability for Highly Automated Driving
Volvo Car Group

4th Scandinavian Conference on System & Software Safety
Stockholm, March 16-17, 2016

ACKNOWLEDGEMENTS:

FUNDED BY SWEDISH PROGRAMME: "FFI-VEHICLE AND TRAFFIC SAFETY"



FUSE

FUnctional Safety and Evolvable architectures for autonomy

Partners: SP, Volvo Cars, KTH, Semcon, Qamcom, Comentor

http://www.fuse-project.se/
rolf.johansson@sp.se

TRUST-ME

Time efficient RobUSt verification of auTonomous vehicles - theory and Methods

Partners: Volvo Cars, Chalmers

jonas.nilsson@volvocars.com

OUTLINE

I. Self-driving vehicles and the DRIVE ME Project
II. New challenges when going autonomous
III. Implications on system design
IV. Implications on system verification
V. Road to autonomy

NOW


San Francisco
ONLY
LANE
600 FEET
San Jose
San Francisco
3 RIGHT LANES

VOLVO

MAIN BENEFITS WITH AUTONOMOUS DRIVING

- Safety
- Environment
- Traffic flow
- Lower and more efficient infrastructure investments
- Use of time

Drive Me

SELF-DRIVING CARS FOR SUSTAINABLE MOBILITY

VOLVO

City of Gothenburg

LINDHOLMEN SCIENCE PARK

TRANSPORT STYRELSEN

TRAFIKVERKET
SWEDISH TRANSPORT ADMINISTRATION

CHALMERS

Autoliv

COOPERATION FOR SUSTAINABLE MOBILITY

- A large-scale test of self-driving vehicles
- Project started Dec 2013
- 100 Volvo cars to selected leasing customers between 2017-2018
- Autonomous Driving (driver not supervising the drive) at selected roads
- Approx. 50 km around Gothenburg

- A world-unique project

A LIMITED SCOPE

Functionality:

- Highly-automated driving on demand
- Certified roads only
- Weather limitations

Road architecture characterized by:

- No oncoming traffic or level crossings
- Pedestrian and bicycle traffic not allowed
- No traffic lights
- Max 70 km/h

THE CHALLENGE

Ambition: Driver out of the loop
(no engineer supervising as in most concept vehicles)

Self-driving vehicles must be able to handle *all* situations
(and *prove* that it can!)

This puts unique requirements on the vehicle,
its sensor, actuators and electrical architecture.

CHALLENGES: FAIL-OPERATIONAL

Auto Pilot fully responsible, once activated

- Cannot rely on driver to take over
- Safe strategy needed for every possible scenario
- Tradeoff between cost and availability

CHALLENGES: WHO IS IN CONTROL?

Two drivers *means Non-traditional ISO 26262 hazards:*

- ***Mode confusion*** – Do driver and car agree on who is in control?
- ***Unfair transitions*** – Is driver/car capable of taking control?
- ***Misuse*** – Does driver or other traffic participants provoke the system?

CHALLENGES: RELATION TO OTHER ITEMS

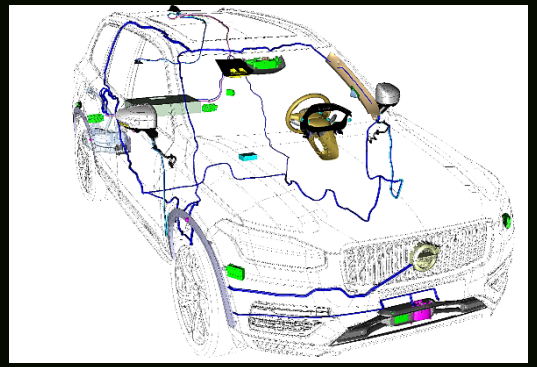
Items outside vehicle

i. Traffic information through cloud
ii. Online map updates

The ITS environment (source: ETSI)

Items in vehicle

i. AD Mode: Faults that the driver will manage
e.g. flat tire
ii. Manual Mode: Added failure modes
e.g. steering commission
iii. Arbitration with other functions
e.g. collision avoidance



CHALLENGES: ENVIRONMENT SENSING

”Old”

- False detections => Unmotivated braking

”New”

- Missed detections => No braking for obstacles
- Localisation error => Run-off road

Situation dependent *– Performance varies heavily between e.g. objects, weather, lighting conditions.*

IMPACTS ON ARCHITECTURE

AD Vehicles require:

- ✓ Redundant sensing
- ✓ Redundant high-end control units
- ✓ Redundant brake system
- ✓ Redundant steering
- ✓ Redundant signaling paths
- ✓ Clustered power distribution
- ✓ Safety critical HMI

IMPACTS ON SENSING

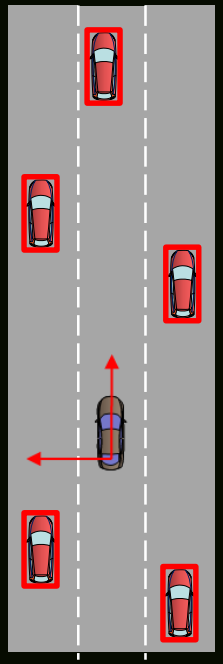
- 1 forward-looking radar
- 4 corner radars
- 2 rear-looking radars
- 3 forward-looking cameras
- 4 surround vision cameras
- 1 forward-looking laser scanner
- Ultrasonic sensors
- Driver Monitor Camera
- Maps and Cloud

SURROUND RADARS AND CAMERAS

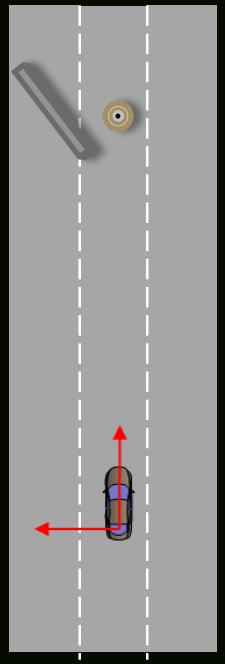
TRI-FOCAL CAM

SENSOR FUSION OBJECTIVES

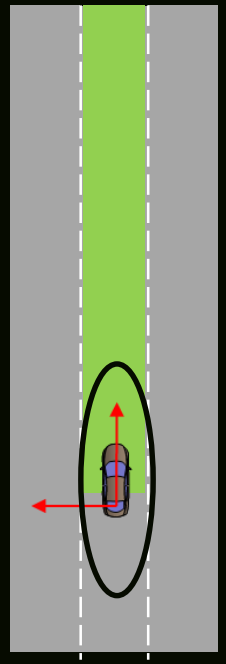
360 degree object detection and mapping



On road obstacle detection

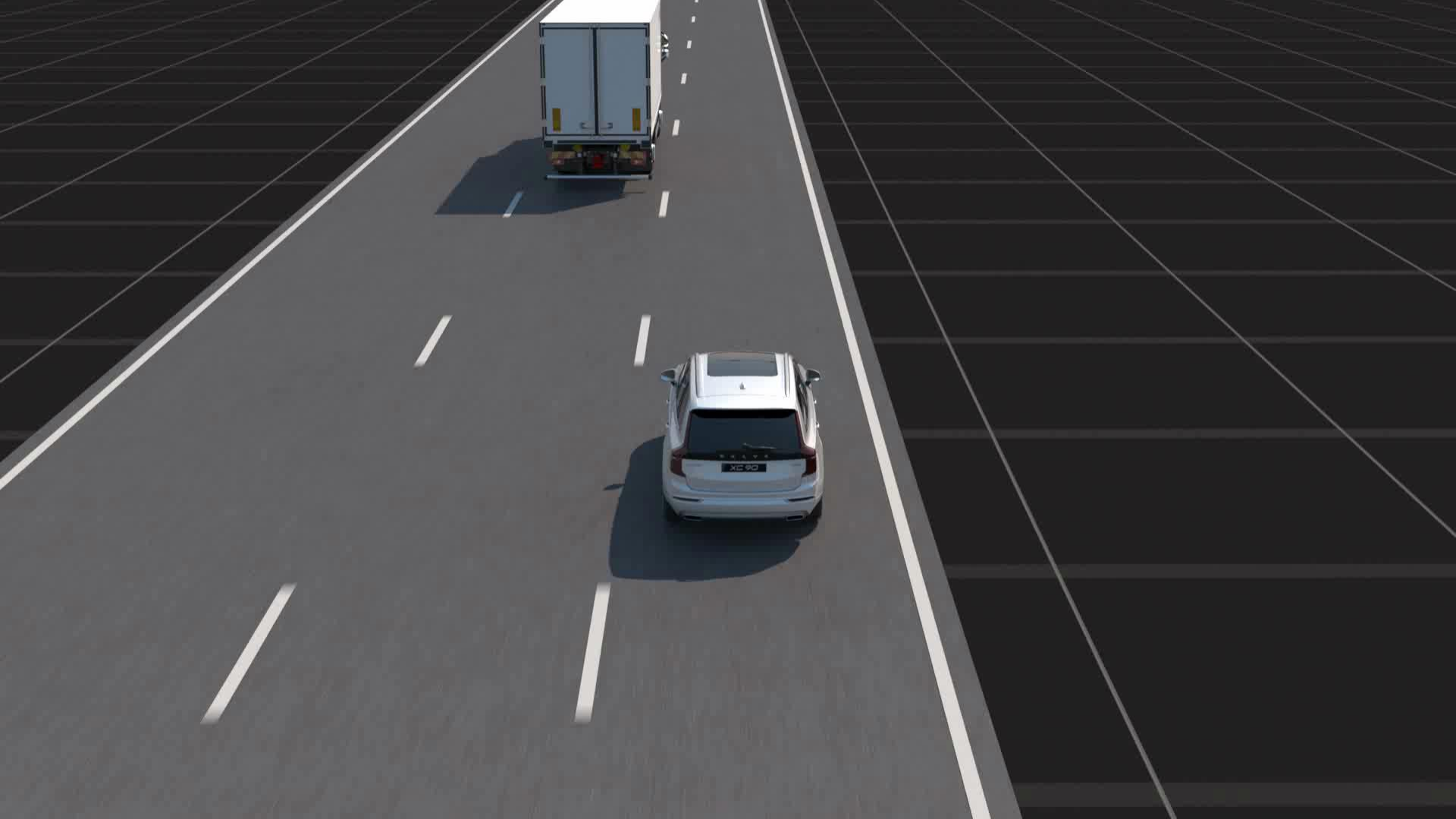


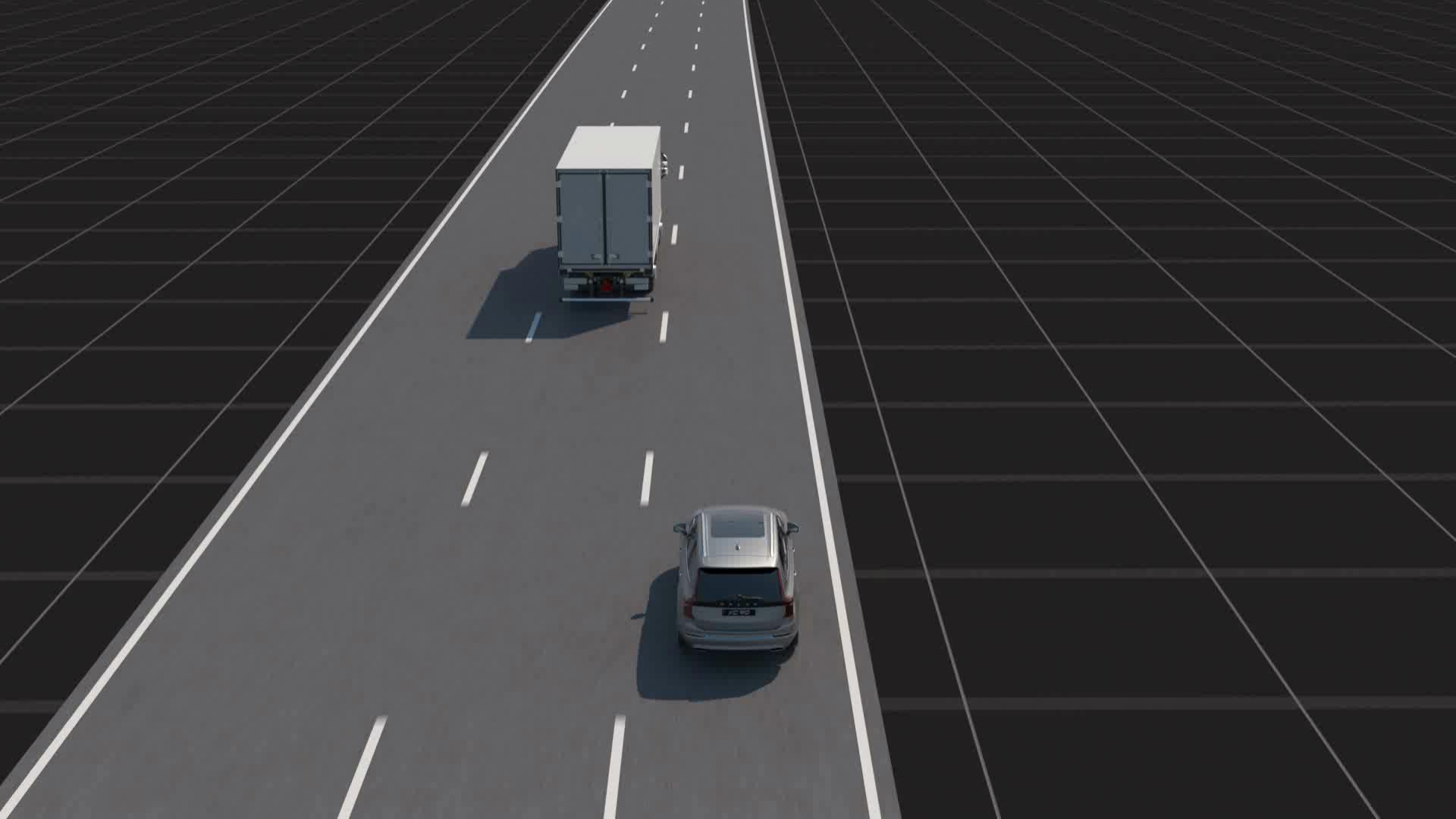
Localization



DECISION-MAKING & THE TROLLEY PROBLEM

*Solution: Drive with **precaution**!*

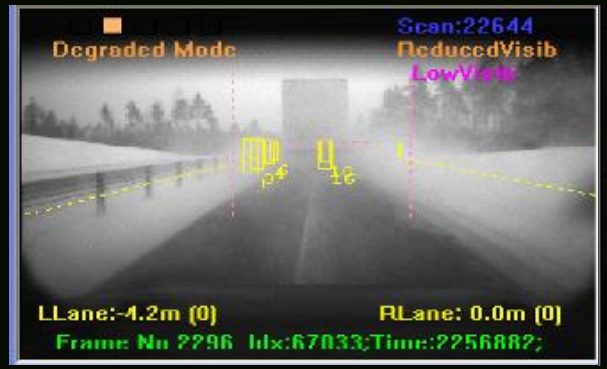

XC 90



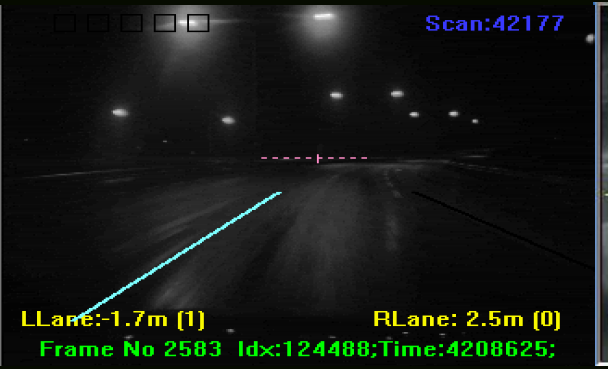
HOW TO VERIFY 10^{-9} FAILURES PER HOUR?

Infeasible to verify by driving billions of kilometers!

ENVIRONMENT SENSING VERIFICATION



Snow smoke



Wet road at night

Low sun

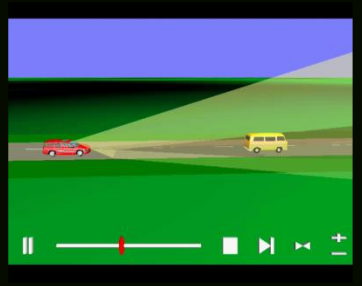
TRAFFIC ENVIRONMENT VARIATIONS

Huge number of traffic scenarios to evaluate!

VERIFICATION STATE-OF-THE-ART

Field Testing
(Real Traffic)

Directed Testing



Simulation

Test Track

VERIFICATION STATE-OF-THE-ART

Active Safety:

- Driver out of the loop only on rare occasions
  e.g. Automatic Emergency Braking (AEB)

Verification Strategy:

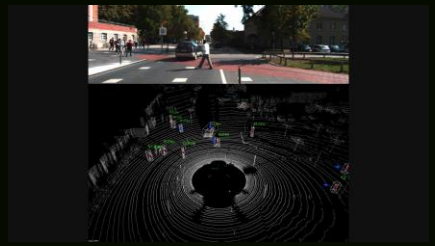
I. Test AEB interventions in ***Directed Testing***
II. Use ***Field Test*** to ensure that false AEB interventions are rare

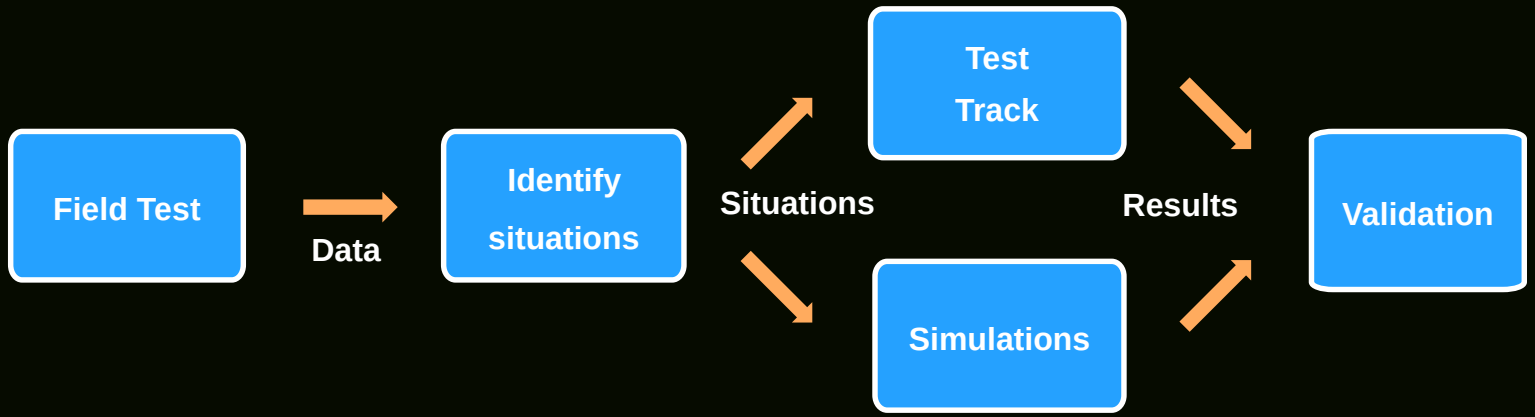
*Only handles a **single** (rare) manuever!*

How can we handle all situations without driving a billion kilometers?

USING DATA MORE EFFICIENTLY

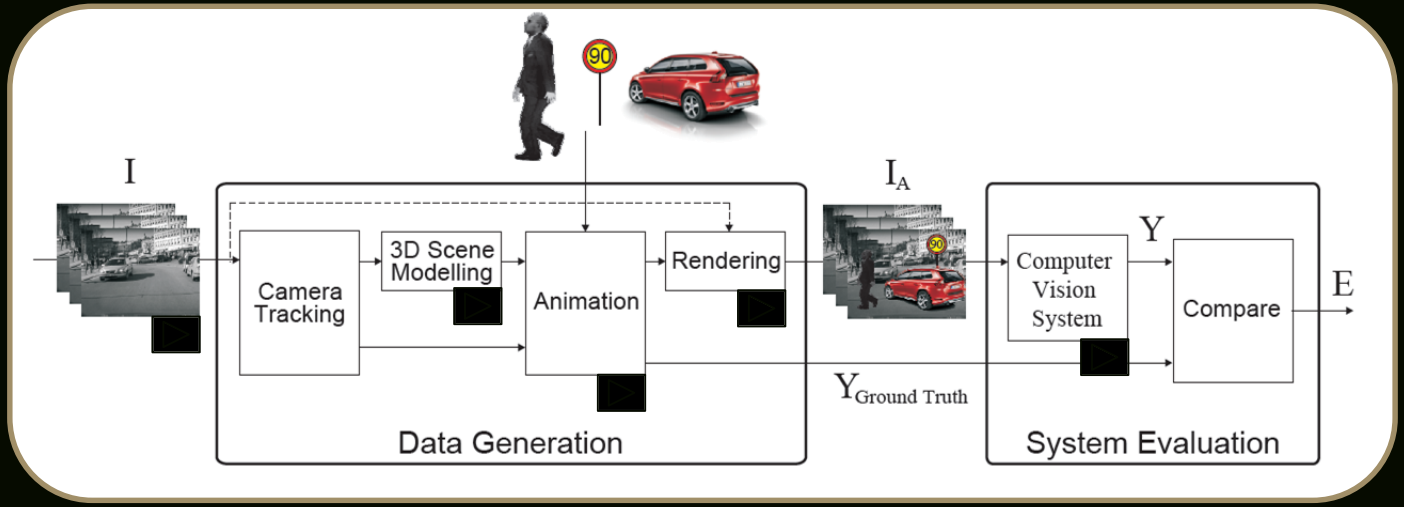
- Crucial to keep field test at feasible size
- Majority of driving is not challenging





CRITICAL SITUATIONS IN SIMULATIONS

Augmented Vision: Photo-realistic virtual objects inserted into real movies



J. Nilsson, A. C. E. Ödblom, J. Fredriksson, A. Zafar, and F. Ahmed, "Performance Evaluation Method for Mobile Computer Vision Systems using Augmented Reality," in *IEEE Virtual Reality Conference*, 2010, pp. 19–22.

J. Nilsson, J. Fredriksson, and A. C. E. Ödblom, "Bundle Adjustment using Single-Track Vehicle Model," in *2013 IEEE International Conference on Robotics and Automation*, 2013, pp. 2888–2893.

CRITICAL SITUATIONS IN SIMULATIONS

TWO ROADS TO AUTONOMY

I. Evolution

- Improve semi-autonomous functionality step-by-step towards full autonomy
- Driver needs to take-over with decreasing frequency
- Driver will be less and less prepared and may one day fail

II. Revolution

- Make a leap towards a fully-redundant system that is better than human driver
- Large development effort, as major impact on vehicle design
- Safety has to be proven with data before deployment

SUMMARY

- ✓ Main drivers for Self-Driving Cars:
  - Use of Time
  - Safety
- ✓ Driver out of the loop is a big change...
- ✓ Fail-operational implies (a lot of) redundancy
- ✓ Verification by merely driving is unfeasible!


DRIVE ME ISN'T JUST THE START OF AN IMPORTANT VOLVO PROJECT –
IT'S THE START OF AN EXCITING FUTURE THAT WILL BRING FREEDOM BACK TO DRIVING.
VOLVO