



# Autonomous vehicle and its challenges

from the computer vision perspective

**Raul Sena Ferreira**

March 23, 2021

# Bio - Currently

Lead data scientist @ **Radix engineering and software - RJ**

PhD student, artificial intelligence @ **LAAS / CNRS - France**

- MSc., systems engineering and computing (PESC) @ **UFRJ**
- BSc., computer science @ **UFRRJ**

Research collaboration with **Fraunhofer institute**, Germany;  
**Jaguar Land Rover**, UK;  
and **UFRRJ**, Brazil

# Bio - Past experiences

## Industry

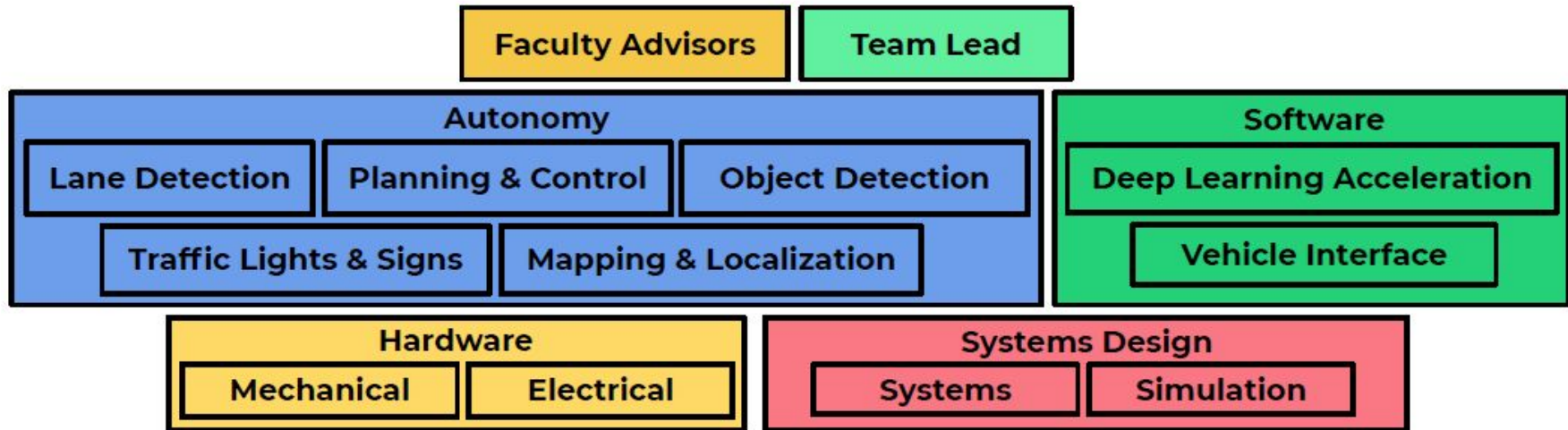
- Machine learning trainer (bootcamp) @ **Vale**
- Technical coordinator @ **IPEA**
- Software engineer @ **Museu Nacional do RJ**
- Software engineer @ **COPPE-UFRJ**

## Academia

- **Ad-hoc reviewer** for Journal of Machine Learning Research (**JMLR**); and International Conference on Fuzzy Systems and Data Mining (**FSDM**)

# Building Autonomous vehicles (AV): a multi-domain task

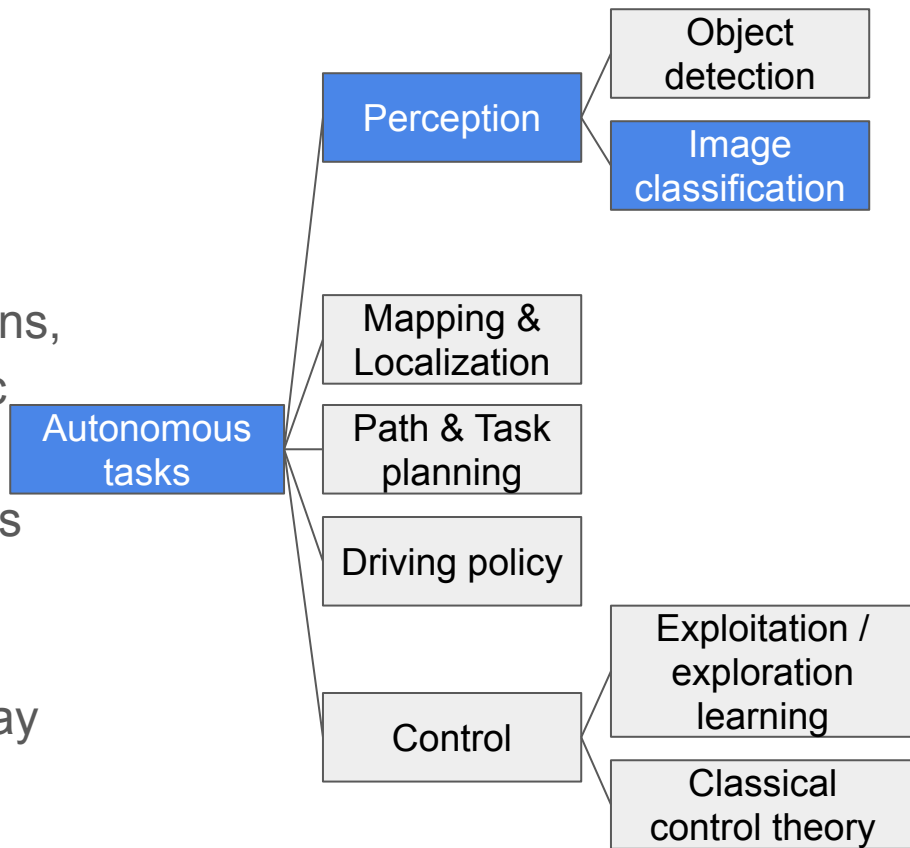
- University of Toronto autonomous vehicle prototype: **built in six months** [1]
- Around 100 students in 12 different subjects [1]



Source: UoT autonomous car team division [1]

# Autonomous tasks

- **Perception:** the “eyes” of the AV
- **Mapping/Localization:** localize traffic signs, allowed street directions, 3D mapings, etc
- **Path/Task planning:** predicts object paths and directions. Execute predefined task
- **Driving policy:** rules to move on a freeway
- **Control:** control speed, steering, etc

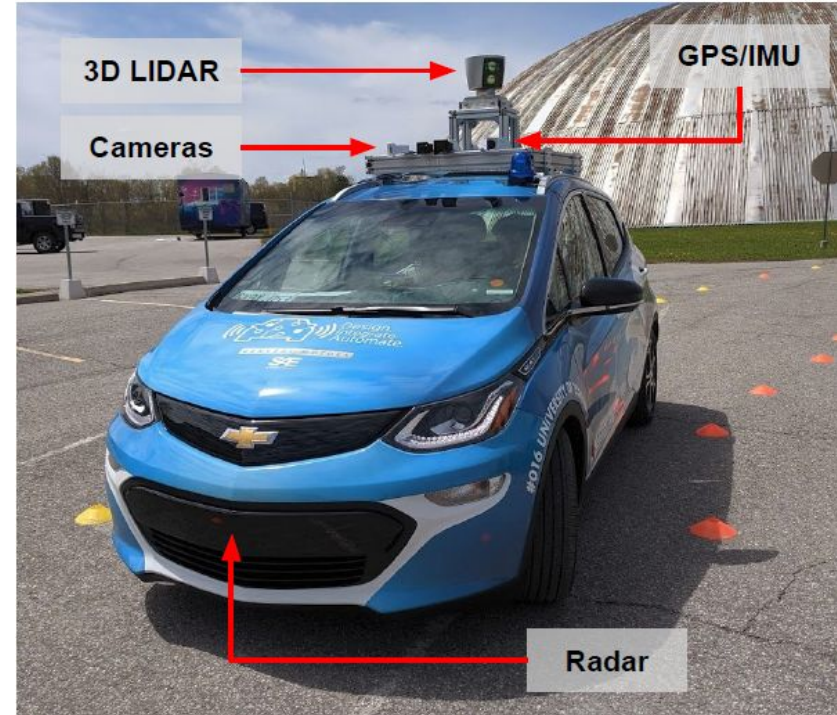


# Sensors: external communication

**Sensors for vision:** LiDAR, Camera, Radar...

**Localization:** Global Navigation Satellite System (GNSS)

**Inertial Navigation System:** position, velocity, accelerometer and gyroscope), Distance Measuring Instruments, etc [29]



Source: Zeus autonomous car [1]

# Sensors: internal communication

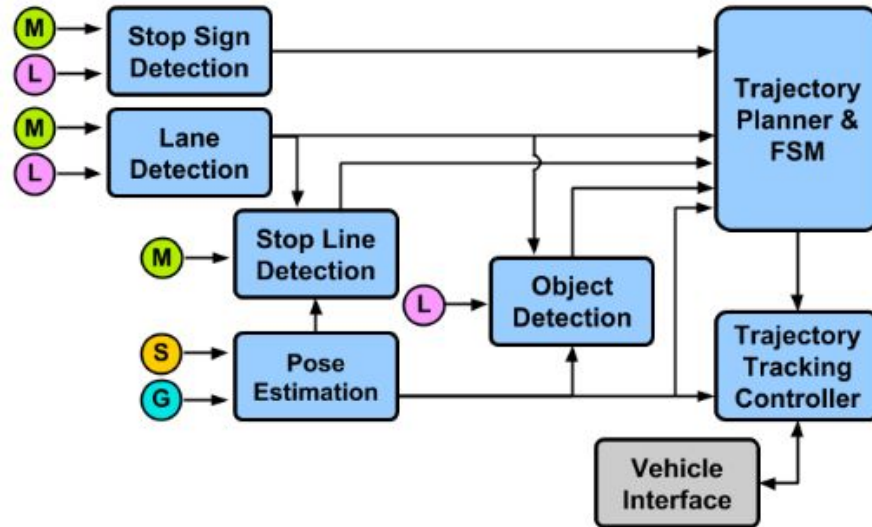
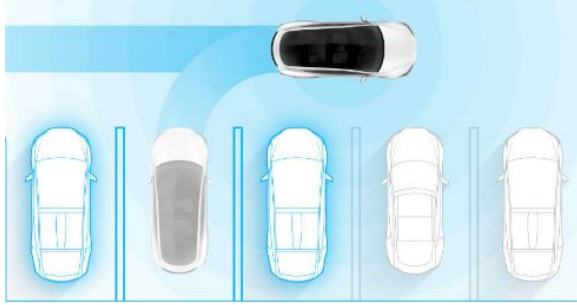


Fig. 2. Our car's software architecture. M: Monocular camera, L: 3D LiDAR, G: GPS/IMU, S: Stereo camera. The Finite State Machine (FSM) determines our current state (lane-keeping | stopping | lane changing).

Source: Zeus autonomous car [1]

# AV performs several different autonomous tasks

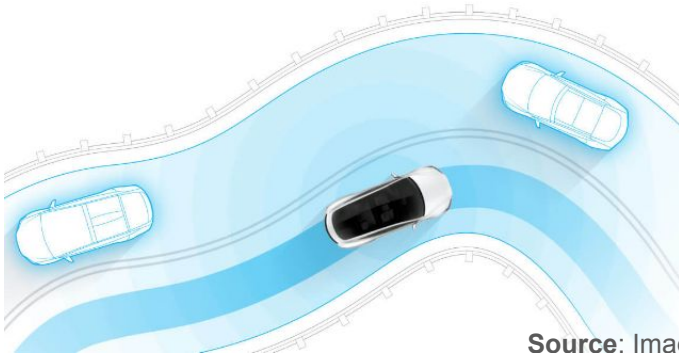
Parking



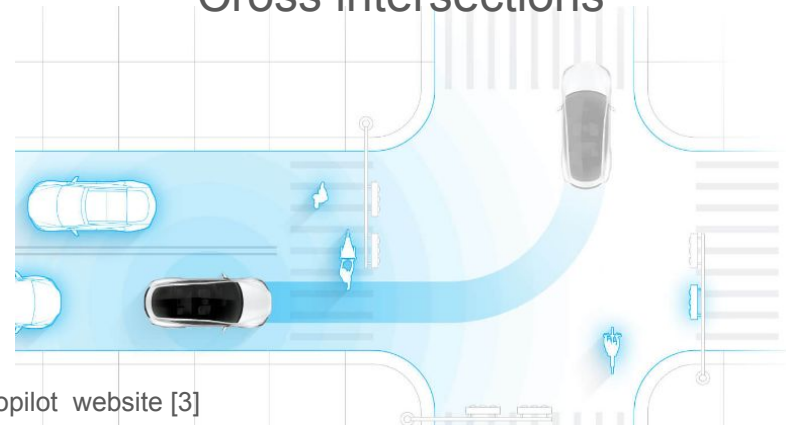
Lane change



Complex navigations



Cross intersections



Source: Images from Tesla autopilot website [3]



# Autonomous vehicles (AV): taking a ride

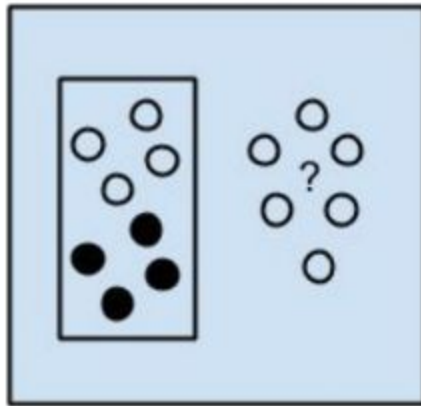


**Source:** Tesla autonomous driving demonstration [3]

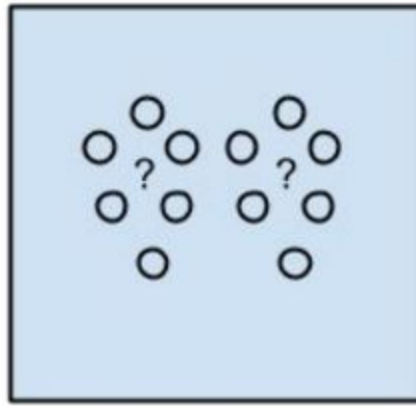
# First things first - What is AI? and ML? and so on...

**Artificial intelligence (AI):** Tries to mimic complex human/nature abilities

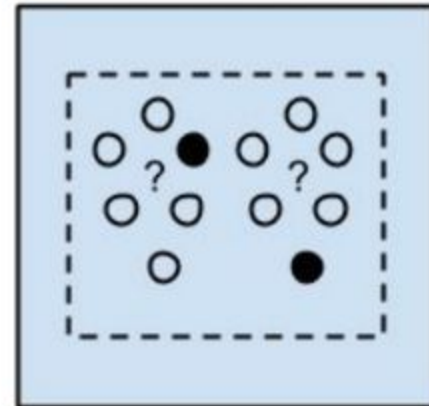
**Machine learning (ML):** AI sub-field algorithms aiming at learning from data



Supervised Learning  
Algorithms



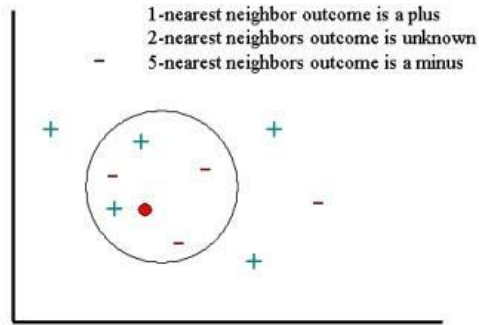
Unsupervised Learning  
Algorithms



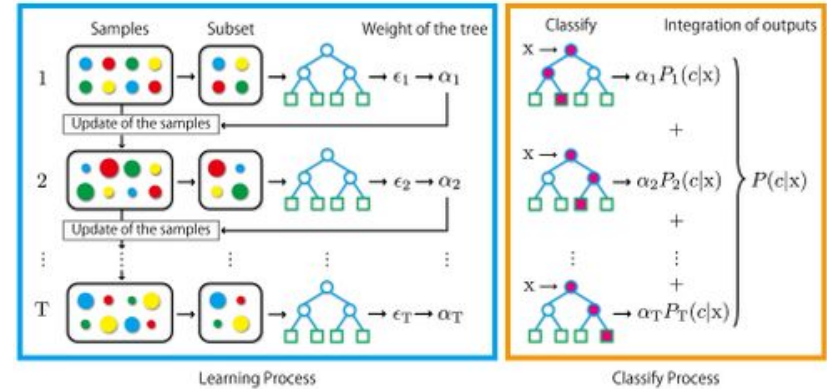
Semi-supervised  
Learning Algorithms

# Machine learning algorithms: some examples

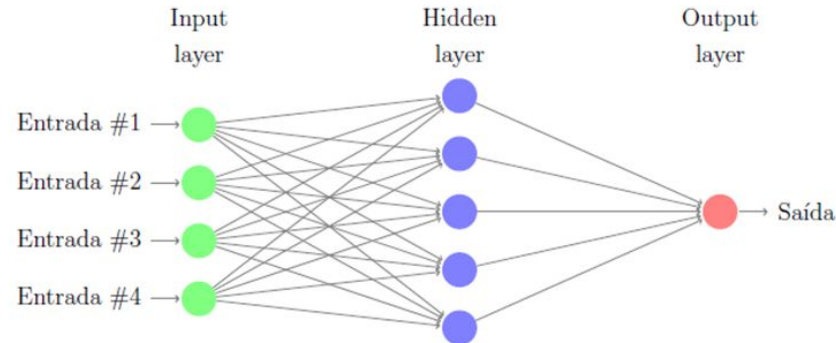
## K-Nearest Neighbors (KNN)



## Random Forests



## Neural Networks

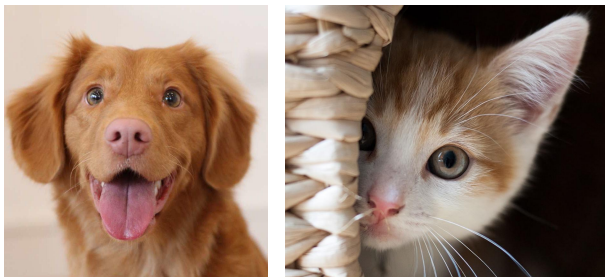


and many others ...

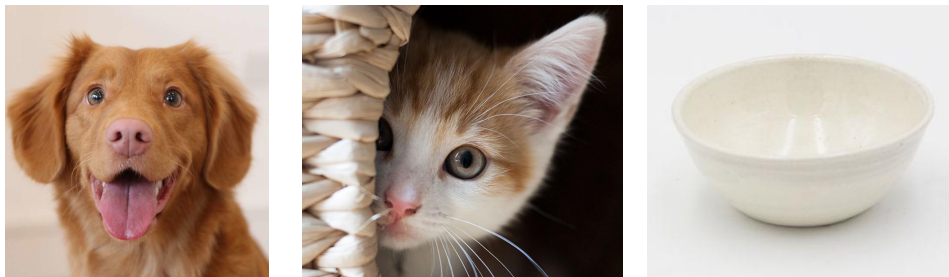
# Machine Learning is a huge research field

There are at least 4 Types of Classification Tasks in Machine Learning [16]

## Binary Classification



## Multi-Class Classification



## Multi-Label Classification

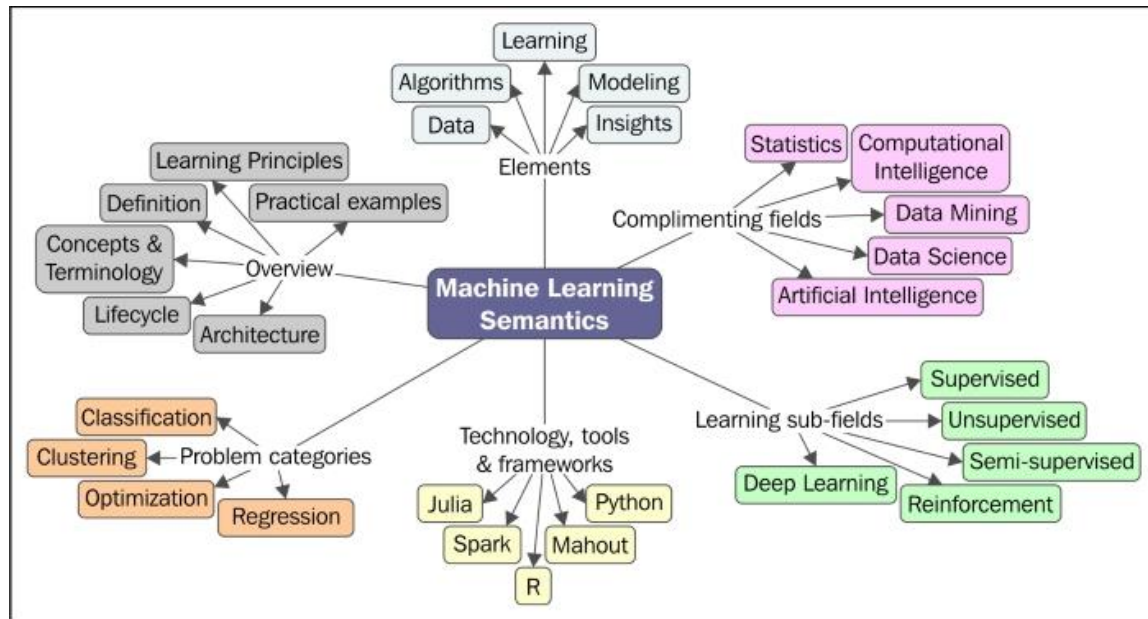


## Imbalanced Classification



# Other ML sub-fields

- Reinforcement Learning
- Self-Supervised Learning
- Inductive Learning
- Deductive Inference
- Transductive Learning
- Active Learning
- Online Learning
- Transfer Learning
- Ensemble Learning



# Deep learning (DL): a subfield of machine learning

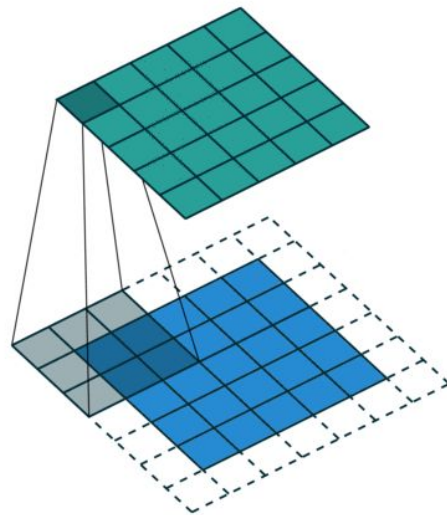
It usually applies Neural Networks in large scale (Deep neural networks - DNN)

**DNN:** a network with a large number of parameters and layers

- Thanks to the increasing computational resources and available data

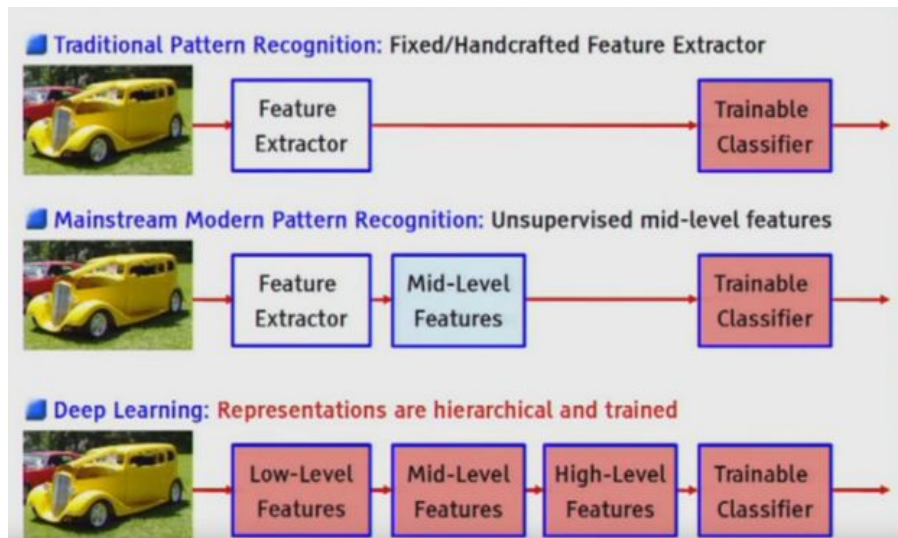
## Four fundamental network architectures:

- Unsupervised Pre-trained Networks
- **Convolutional Neural Networks**
- Recurrent Neural Networks
- Recursive Neural Networks



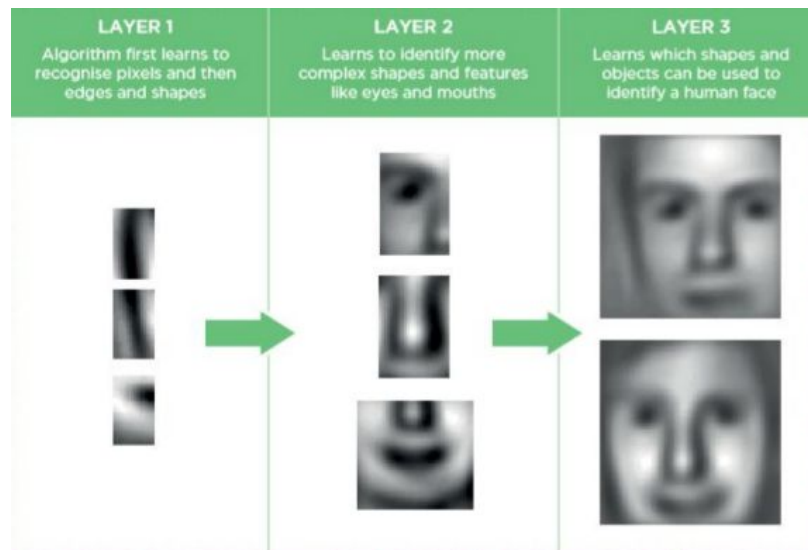
# DL capabilities

## All-in-one pipeline



Source: Yann LeCun [4]

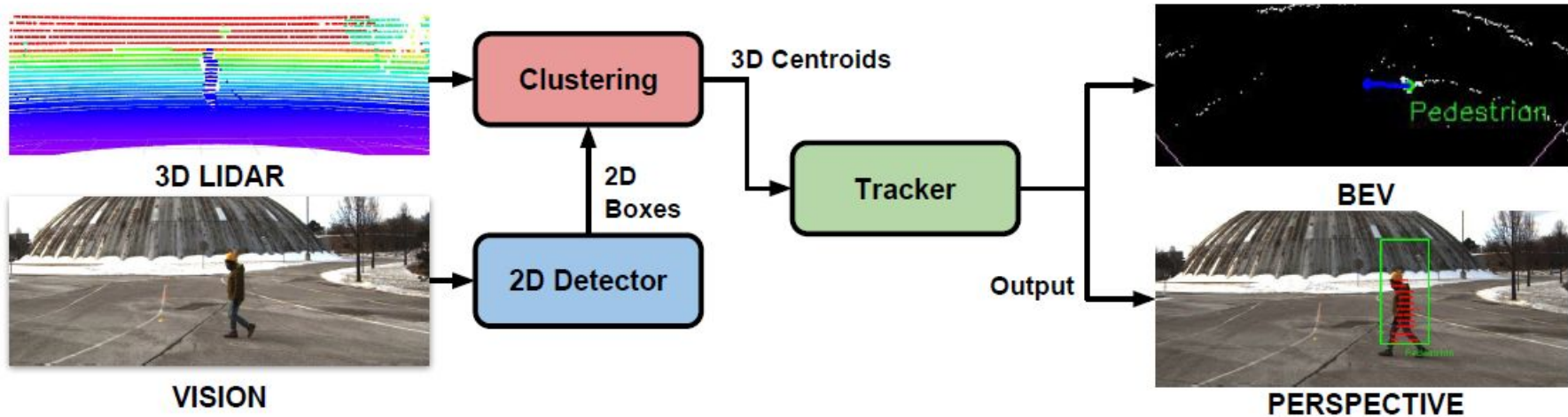
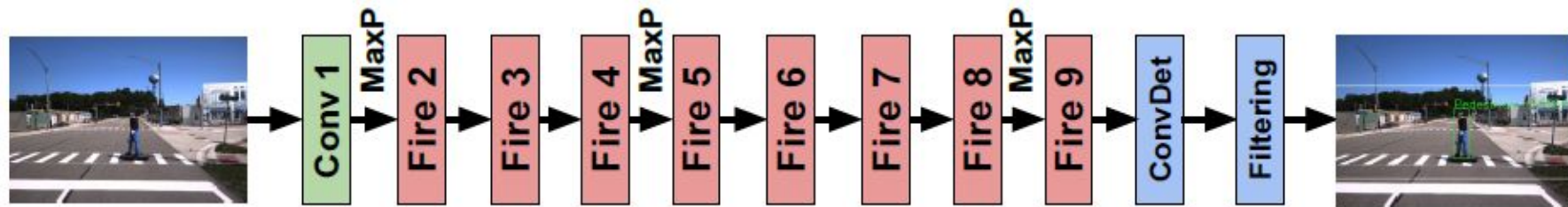
## Low to High level representations



Source: Why DL is needed ? [5]



# DL applied to AV: object-recognition example



Source: Zeus: A System Description of the Two-Time Winner of the Collegiate SAE AutoDrive Competition [2]



# DL is a strong and useful technology, however ...

**DL is not trustworthy for such critical scenarios (there are 3 main reasons):**

- **Design errors:** ML model inaccuracies (all models are imperfect)
- **Data incompleteness:** insufficient test coverage and incomplete learning
- **Environment oversimplification:** unseen interactions, behaviors or problems

# Challenge #1: 99% of accuracy is not enough

## 99% of accuracy is not enough

- 1% of wrong decisions can be catastrophic (people inside or outside the car)



**Source:** Tesla model X fatal crash [6]

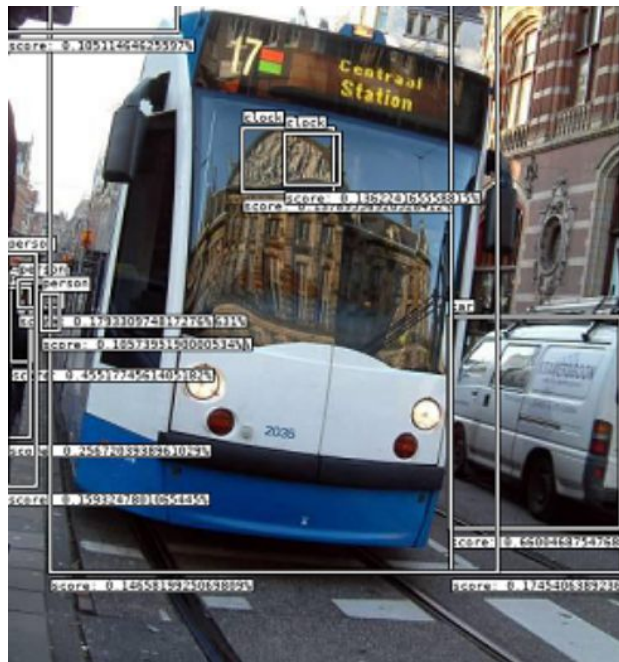


**Source:** Uber deadly crashes a cyclist [7]

# Unexpected objects and situations in the environment

Is there a clock tower in front of the vehicle or is the vehicle in front of a tram ?[14]

Different objects with the same intention (Figure 2) or not (Figure 3) [15]



## Challenge #2: ML threats that mislead DNN decisions

**Distributional shift:** data distribution changes while ML model is online [8]

**Anomalies:** identification of an anomalous input or behavior [9]

**Adversarial examples:** perturbations that lead to misclassifying known inputs [10]

**Class novelty:** classes of unseen objects during the ML model building

**Noise:** small dysfunctions and/or information loss

# Adversarial examples

They can be intentional attacks or natural consequence of the environment [10]

panda gibbon (99.3%)

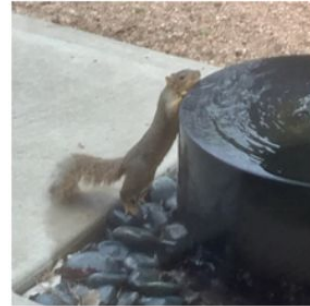


(a) Perturbations in digital world.



(b) Perturbations in real world.

fox squirrel sea lion (99%)



(c) Without perturbations, natural example.

**Example:** Stop sign is recognized as a 45 speed limit sign [12]



# Distributional shift

Distributional differences between training data and data at runtime

$$\exists X : P_{t0}(X, y) \neq P_{t1}(X, y)$$

**Ex: Deteriorate traffic sign images, degraded perception or other changings in the characteristics of the objects**



Each image on the left is original and on the right the deteriorated or different version



# Anomaly images

Some examples of anomalous images in an autonomous vehicle camera [13]



Example of a Fault in the Clock System



Color Error due to an Image Pipeline Fault

# Novelty classes

DNN can be exposed to new and relevant objects for its domain [11]



(a) Correct detection and braking.



(b) Misclassification and collision.

**Source:** Emergency braking system for an unexpected class object (cow) [11]



# How to overcome these challenges ?

How to **assure that the DNN is giving the right decision** at runtime ?

After the detection, how do **we should react** ?

**Very active and interdisciplinary research field in Europe**

# References

- [1] Burnett, K., Schimpe, A., Samavi, S., Gridseth, M., Liu, C. W., Li, Q., ... & Schoellig, A. P. (2019, May). Building a winning self-driving car in six months. In 2019 International Conference on Robotics and Automation (ICRA) (pp. 9583-9589). IEEE.
- [2] Burnett, K., Qian, J., Du, X., Liu, L., Yoon, D. J., Shen, T., ... & Zhang, K. (2020). Zeus: A System Description of the Two-Time Winner of the Collegiate SAE AutoDrive Competition. arXiv preprint arXiv:2004.08752.
- [3] Tesla autopilot website. Url: <https://www.tesla.com/autopilot> Accessed in 2020/05/31.
- [4] Yann LeCun, learning hierarchical features, slides, all rights reserved
- [5]<https://towardsdatascience.com/why-deep-learning-is-needed-over-traditional-machine-learning-1b6a99177063>
- [6] Tesla X model accident. URL: <https://www.teslarati.com/tesla-statement-fatal-model-x-crash-ntsb-investigation/>
- [7] Uber deadly hits a cyclist URL: <https://pro.largus.fr/actualites/un-vehicule-autonome-duber-implique-dans-un-accident-mortel-9061390.html>
- [8] Ferreira, R. S., Zimbrão, G., & Alvim, L. G. (2019). AMANDA: Semi-supervised density-based adaptive model for non-stationary data with extreme verification latency. Information Sciences, 488, 219-237.
- [9] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM computing surveys (CSUR) 41.3 (2009): 1-58.

# References

- [10] Yuan, X., He, P., Zhu, Q., & Li, X. (2019). Adversarial examples: Attacks and defenses for deep learning. IEEE transactions on neural networks and learning systems, 30(9), 2805-2824.
- [11] Dreossi, T., Donzé, A., & Seshia, S. A. (2019). Compositional falsification of cyber-physical systems with machine learning components. Journal of Automated Reasoning, 63(4), 1031-1053.
- [12] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., ... & Song, D. (2018). Robust physical-world attacks on deep learning visual classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1625-1634).
- [13] Evaluating Functional Safety in Automotive Image Sensors, Semiconductor Components Industries, LLC, Report. May 2018. URL: <https://www.onsemi.cn/pub/Collateral/TND6233-D.PDF>
- [14] Mirror, mirror on the wall... AI (Deep Learning) needs to learn it all. URL: <https://medium.com/@harshaangeri/mirror-mirror-on-the-wall-ai-deep-learning-needs-to-learn-it-all-ad221bd399e1>
- [15] ANDREJ KARPATHY, AI for Full Self-Driving. ScaledML conference. URL: <https://info.matroid.com/scaledml-media-archive-2020>
- [16] <https://machinelearningmastery.com/types-of-classification-in-machine-learning/>

# Thank you

Website: [www.raulferreira.com.br](http://www.raulferreira.com.br)

Email: [rsenaferre@laas.fr](mailto:rsenaferre@laas.fr)

LinkedIn: <https://www.linkedin.com/in/raulsenaferreira/>