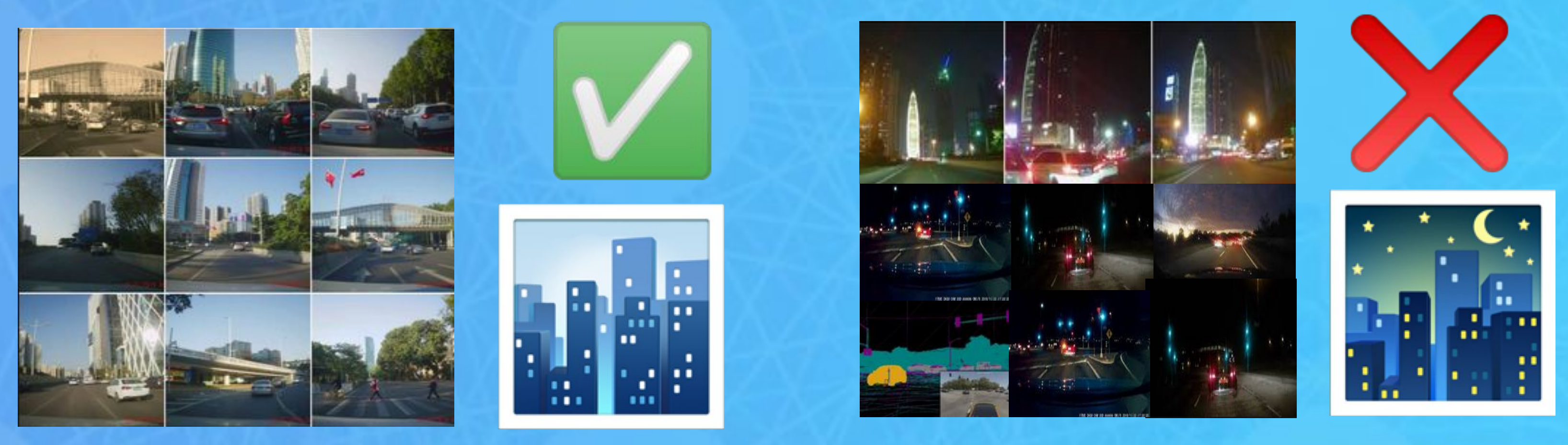
Improving the performance of Deep-Neural-Network-Controlled **Automatic** Driving Systems (ADS) In Unseen Lighting Conditions

The **end-to-end** pipeline is the neural network approach to ADS. It uses **convolutional neural networks (CNNs)** to operate the vehicle. Research shows that CNNs trained using synthetically **augmented datasets** are more resilient to unseen conditions.

Problem

CNNs **tend to overfit to the training data.** It performs well in the conditions exposed during training, but **does not** in **never-seen-before** lighting conditions.



A CNN model trained with images collected during the daytime might perform well in daylight but underperform at night.

Hypothesis

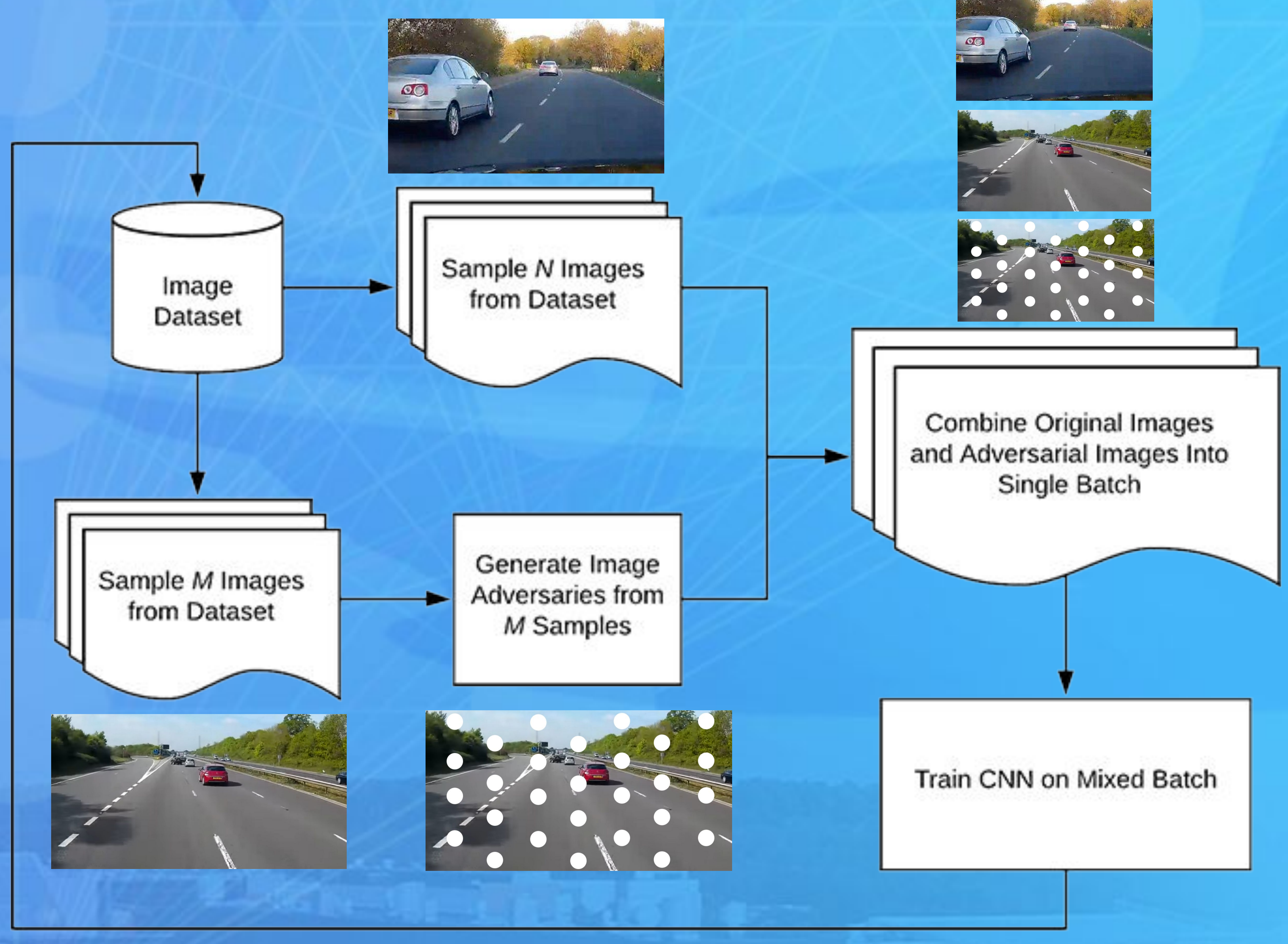


Image Dataset
Sample *N* Images from Dataset
Sample *M* Images from Dataset
Generate Image Adversaries from *M* Samples
Combine Original Images and Adversarial Images Into Single Batch
Train CNN on Mixed Batch

(Rosebrock, 2021)

Research suggests that CNNs trained with synthetically **augmented datasets** including a mix of normal and corrupted images will perform better in unseen conditions than CNN models trained with standard procedures.

Goal

To improve the performance of CNN models in unseen lighting conditions.

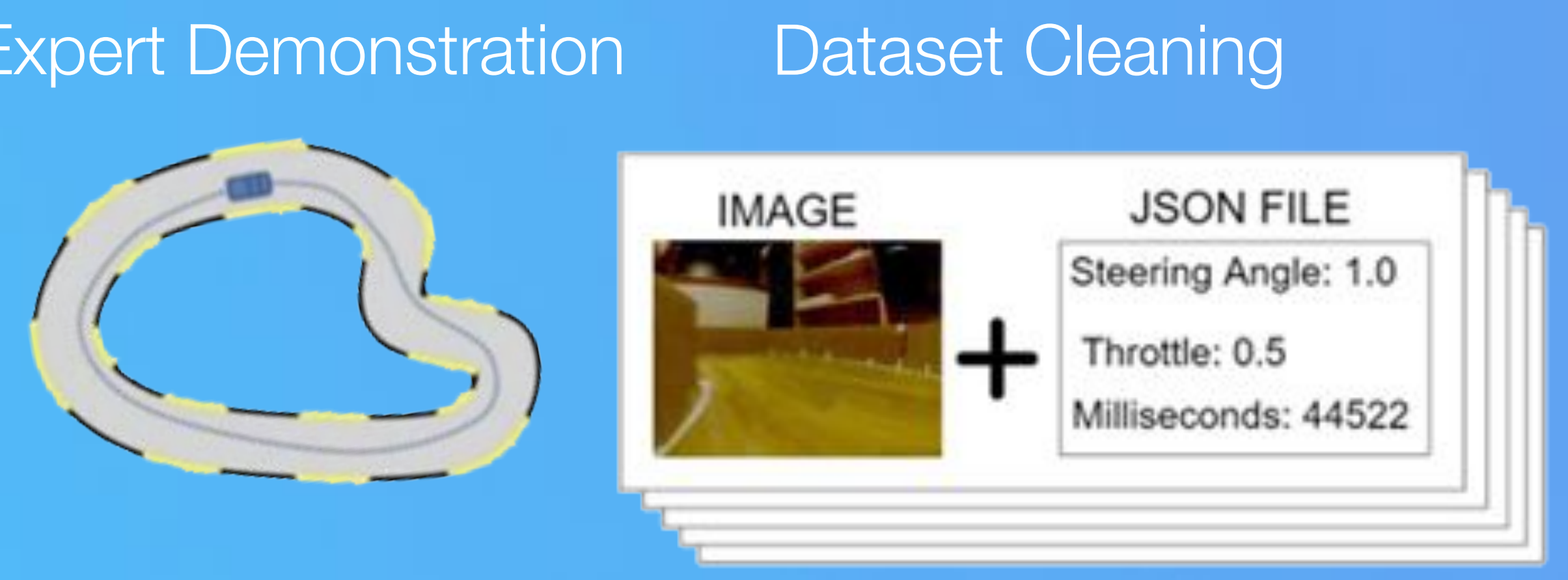
Research Question

Can **adversarial defense** training methods **improve** the neural network **generalization skills** to unseen **lighting conditions?**

Method

1 Collect Labelled Dataset

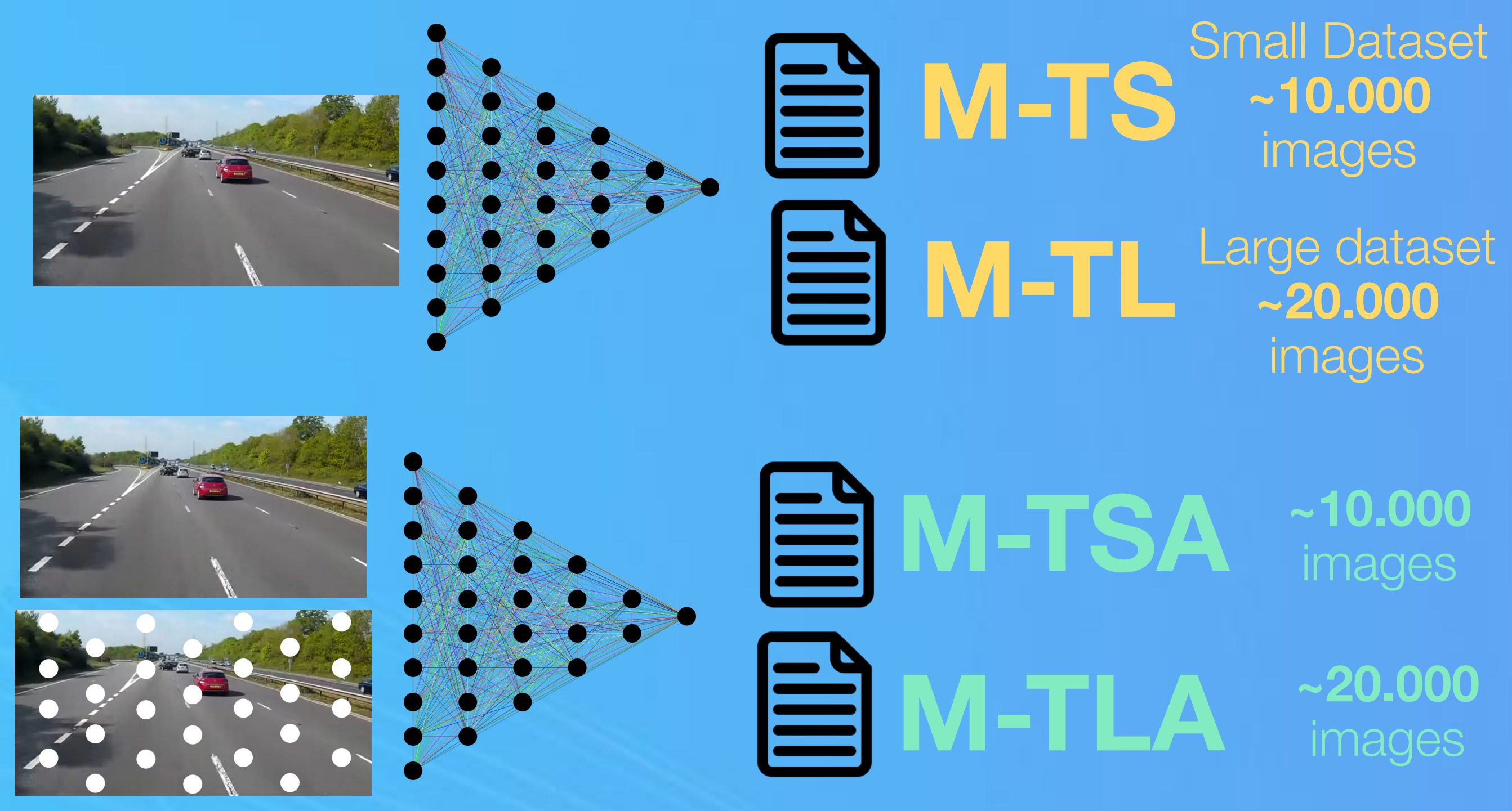
Imitation Learning
Driving by example



Steering Angle: 1.0
Throttle: 0.5
Milliseconds: 44522

2 Train CNN Models

Use the dataset to create models using different training methods.

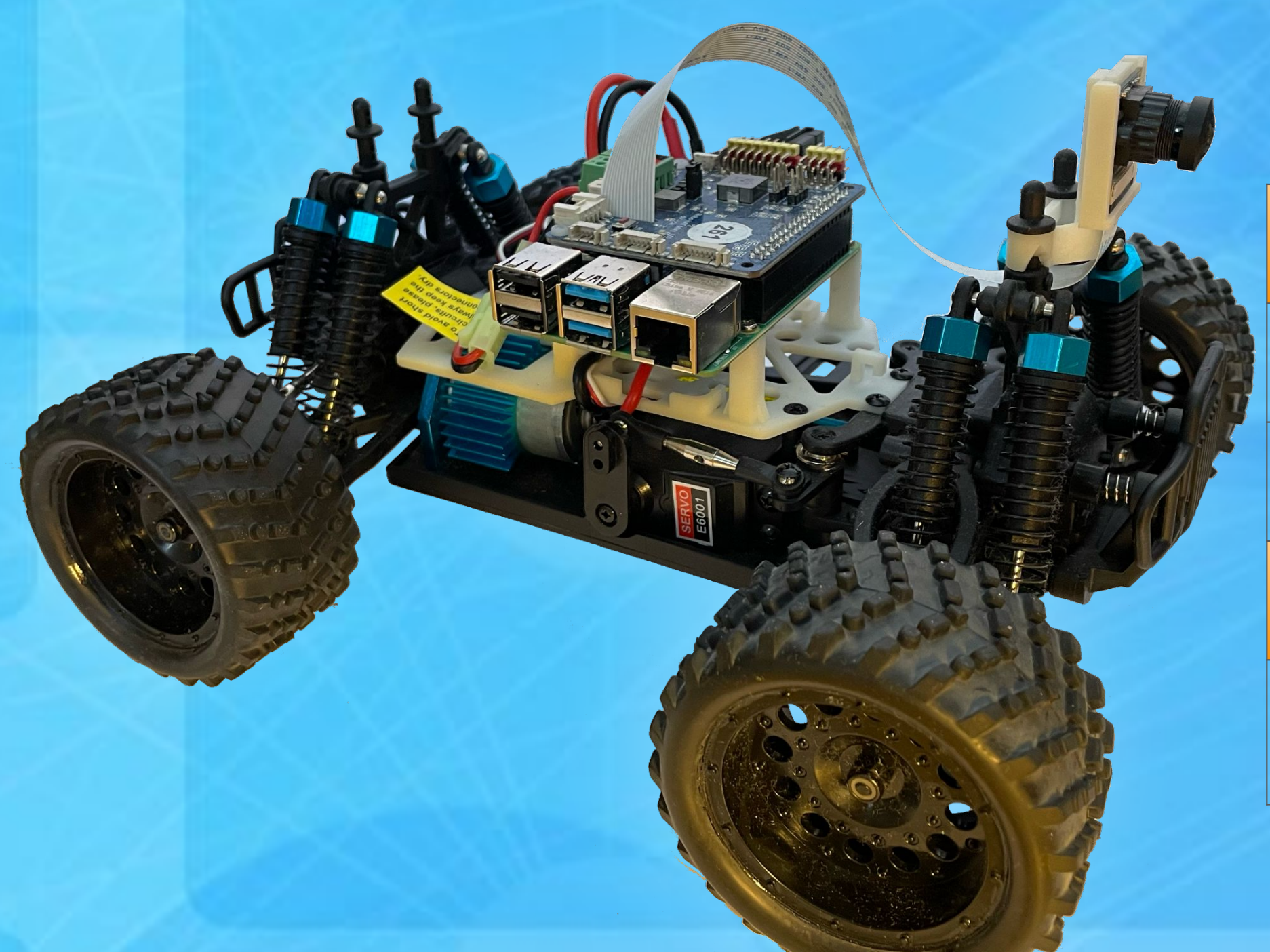


Standard training

Adversarial Training (Rosebrock, 2021)

3 Deploy and Evaluate

Deploy the models in a scaled real-world setup and evaluate their performance for two laps both in seen and unseen conditions.



Evaluation conditions

Independent variables	Values
Laps	**2**
Lights	**low, high**
Dependent variable	Values
Collisions	**[0...n]**

Results

Collisions in **2 laps**

Model training method		Seen Lower-lights	Never-seen-before Higher-lights
Standard ❌ Have collisions In higher lights	**M-TS**	✅ 0	❌ 5
	M-TL	✅ 0	❌ 4
Proposed ✅ Collision free in both conditions	**M-TSA**	✅ 0	✅ 0
	M-TLA	✅ 0	✅ 0

Answer to the **Research Question**

Yes, it can.
Adversarial methods can improve the CNN performance in unseen lighting conditions.

Mike Camara
Ms Software Engineering

Dietmar Pfahl, PhD
Supervisor

See the video of the experiment on **youtu.be/A_dHfvMgd-w**

Visit the **repository** for the entire **thesis**, **code**, and **references** on **github**.com/mikecamara/adversarial-machine-learning-attacks

UNIVERSITY OF TARTU
Institute of Computer Science
1632

TAL TECH