SMILIES
reSilient coMputer archItectures
and LIfE Sciences

Politecnico
di Torino
Department of Control and
Computer Engineering

DAUIN

CARACAS: vehiCular ArchitectuRe for detAiled CAN Attacks Simulation

SADEK MISTO KIRDI, **NICOLA SCARANO**, FRANCO OBERTI, LUCA MANNELLA,
STEFANO DI CARLO, ALESSANDRO SAVINO

POLITECNICO DI TORINO, ITALY

VEHICLES IN THE 21ST CENTURY

Changes in the automotive ecosystem

Transition towards electric vehicles:

Shift in drivers of innovation: Battery Electric Vehicles

Massive use of electronics components

ECUs oversee various key operations

Increased communication and automation

E.g., ACC, CACC, V2V

Affecting the attack surface of the vehicles

CAN NETWORK AND SECURITY ISSUES

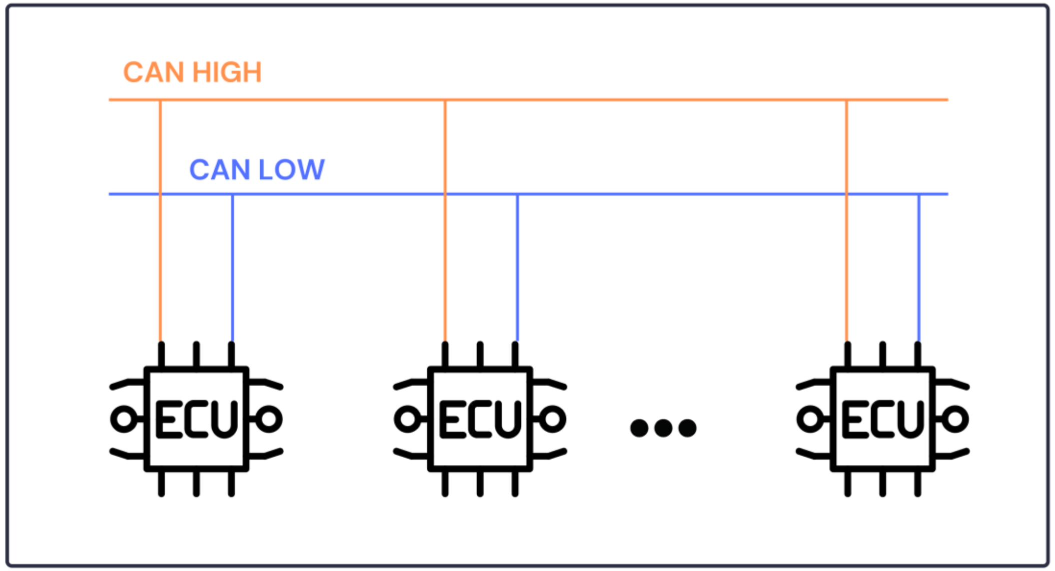
Controller Area Network (CAN): backbone

- Enable massage transmission among various components

  E.g., ECUs, sensors and intelligent actuators;

But... CAN bus external accessibility

- allows attackers with multiple **exploitation opportunities**
- an adversary may critically manipulate the vehicle behavior by **injecting** malicious **packets**



CAN NETWORK AND SECURITY ISSUES

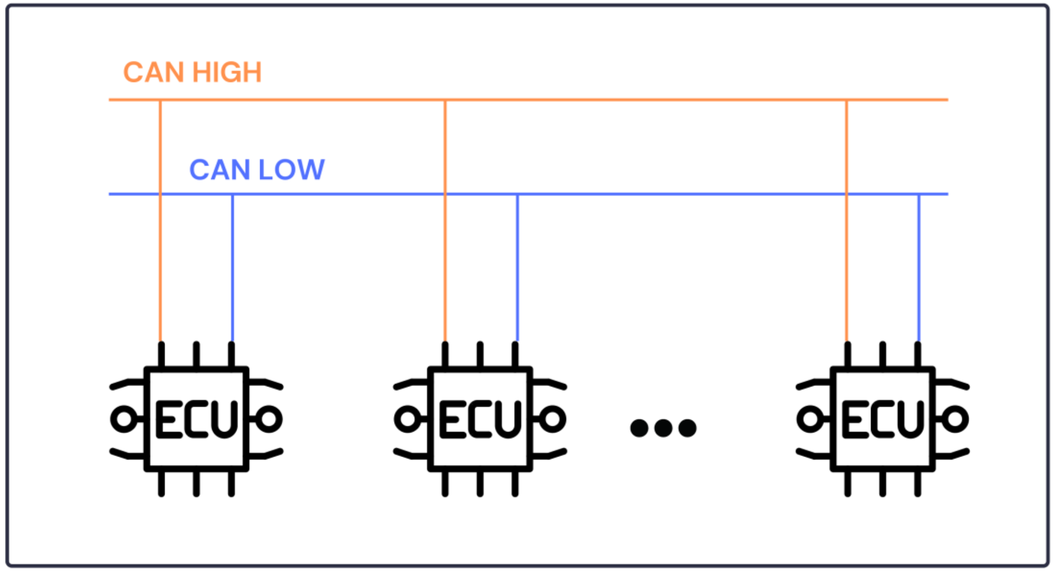
Controller Area Network (CAN)

- Enable massage transmission among various components ECUs

  E.g., sensors and intelligent actuators;

CAN bus external accessibility

- allows attackers with multiple **exploitation opportunities**
- an adversary may manipulate the system by **injecting** malicious **packets**



Attacks examples

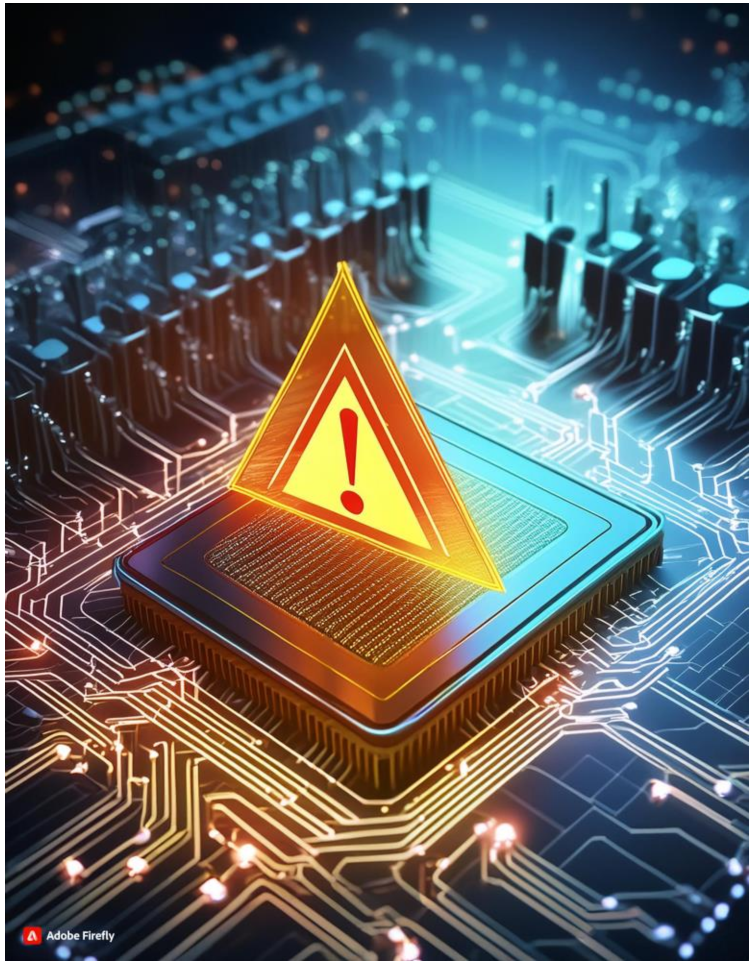
- Shut off the engine
- Turn off the immobilizer
- Engine torque modification

IDS: A PROMISING SOLUTION

Intrusion Detection Systems are countermeasures of great interests for CAN security:

- Often powered by AI
- Simple and efficient
- Monitoring of network or device activity;
- Raising alarms when unexpected events occurs;

Multiple studies have presented promising results in *Automotive applications*



THE NEED FOR DATA

On the other hand, CAN IDSs research presents challenges in **replicating and comparing** methodologies due to difficulties in the experiment set up

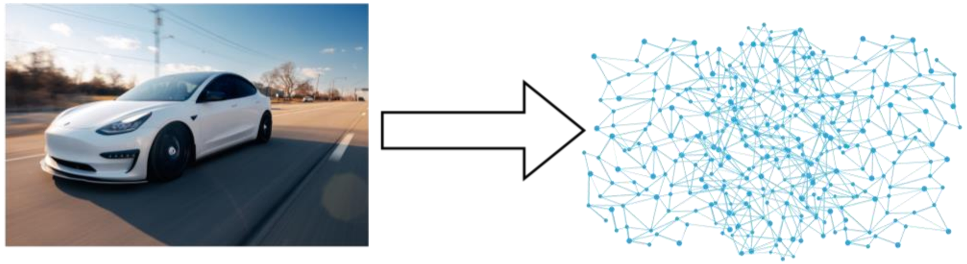
Over time, effort to generate **datasets** to provide researchers with CAN data for testing

Real world dataset

Large collection of accurate CAN data while driving

<u>Data collection problem</u>:

- Time consuming and expensive
- Limited number of vehicles and the range of attacks



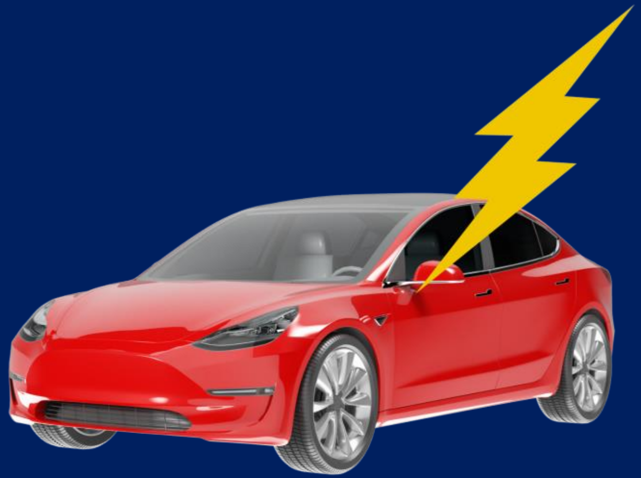
SIMULATION APPROACH

Synthetic dataset

- Simulate:
  - CAN bus environment
  - Regular and malicious signals traffic
- Pros:
  - Reduce time and cost of CAN data acquisition
  - Easy to generate large amount of data to train ML based IDSs

PROBLEM

- Lack of verification of physical effects of attacks
- Doubts about on the consequences of the attacks



CARACAS: vehiCular ArchitectuRe for detailed CAN Attacks Simulation

Components

- Vehicle dynamics
- Integrated CAN bus model
- CAN injection module

Capabilities

- Generation of regular CAN traffic and malicious CAN messages
- Simulation of effect of attacks vehicle's operational condition

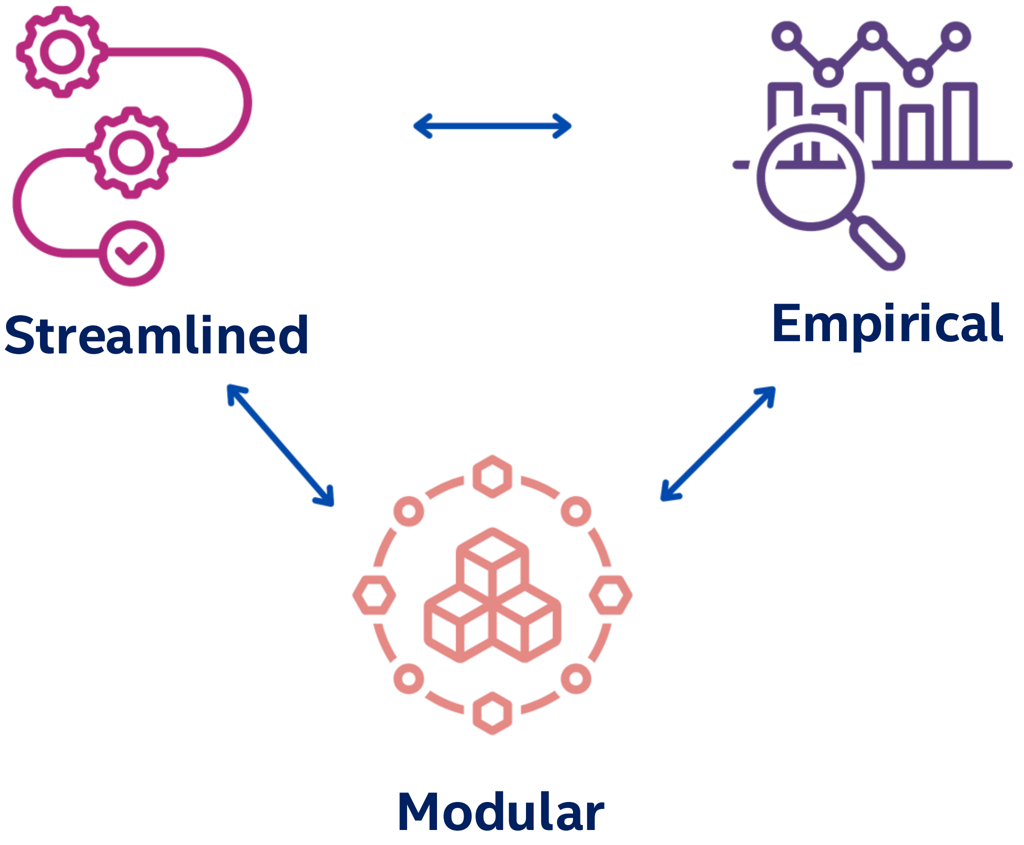
CARACAS: vehiCular ArchitectuRe for detailed CAN Attacks Simulation

Components

- Vehicle dynamics
- Integrated CAN bus model
- CAN injection module

Capabilities

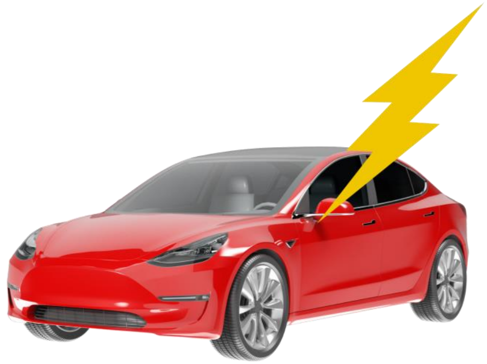
- Generation of regular CAN traffic and malicious CAN messages
- Simulation of effect of attacks vehicle's operational condition



BEYOND THE ARCHITECTURE: A REAL USE CASE

Implemented

BEVs vehicle dynamics of **Tesla Model 3**



Tested

Injecting malicious **torque messages**

Analyzed

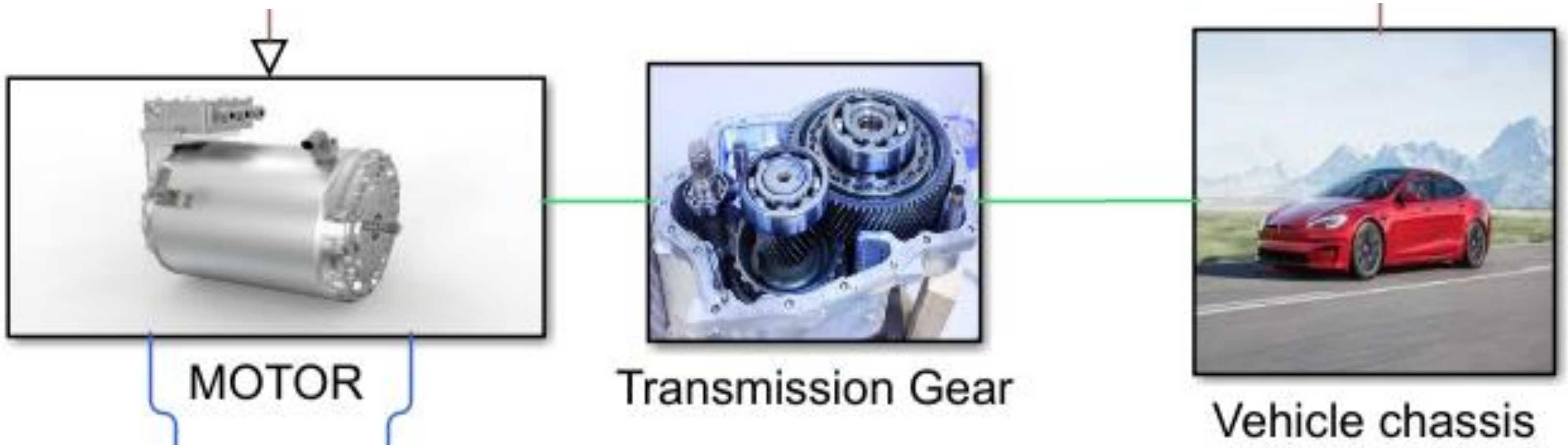
The performance on two driving scenarios:

- **Extra Urban Driving Cycle**
- **Cruise Mode**

BEVS DYNAMIC MODEL

Integrate essential vehicle's components:

- Chassis: structural backbone, physical attributes
- Electric motor and transmission gear focused on performance and interaction with vehicle powertrain

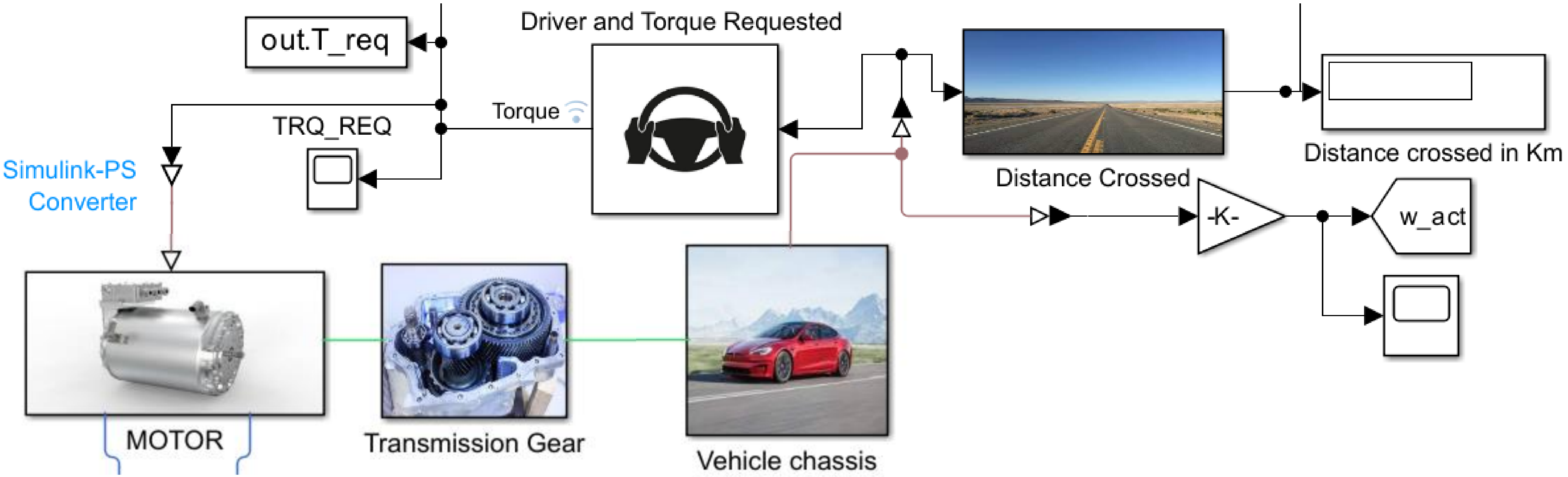


BEVS DYNAMIC MODEL

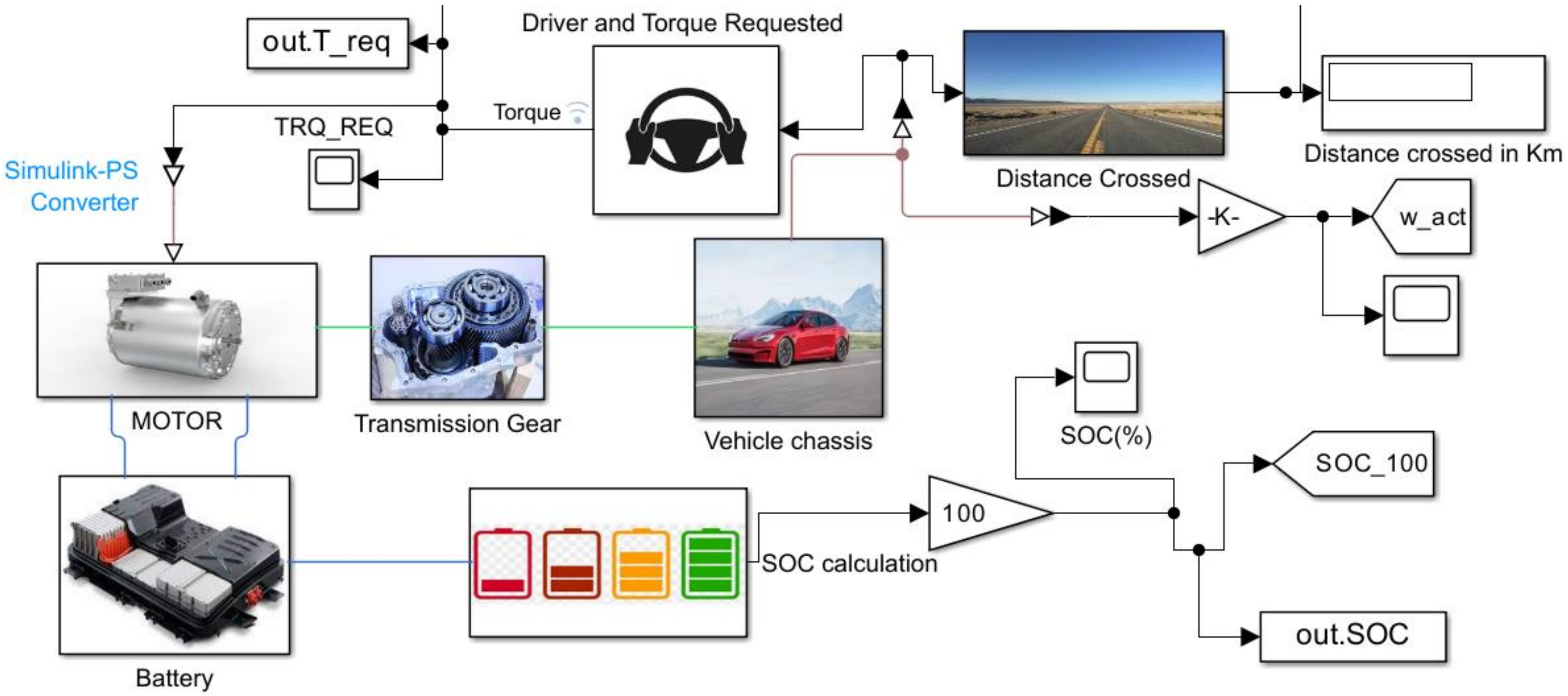
Vital paramemeter of the motor: **Torque**

Amount of rotational force the motor develop

Responsible for breaking and accelerating



BEVS DYNAMIC MODEL



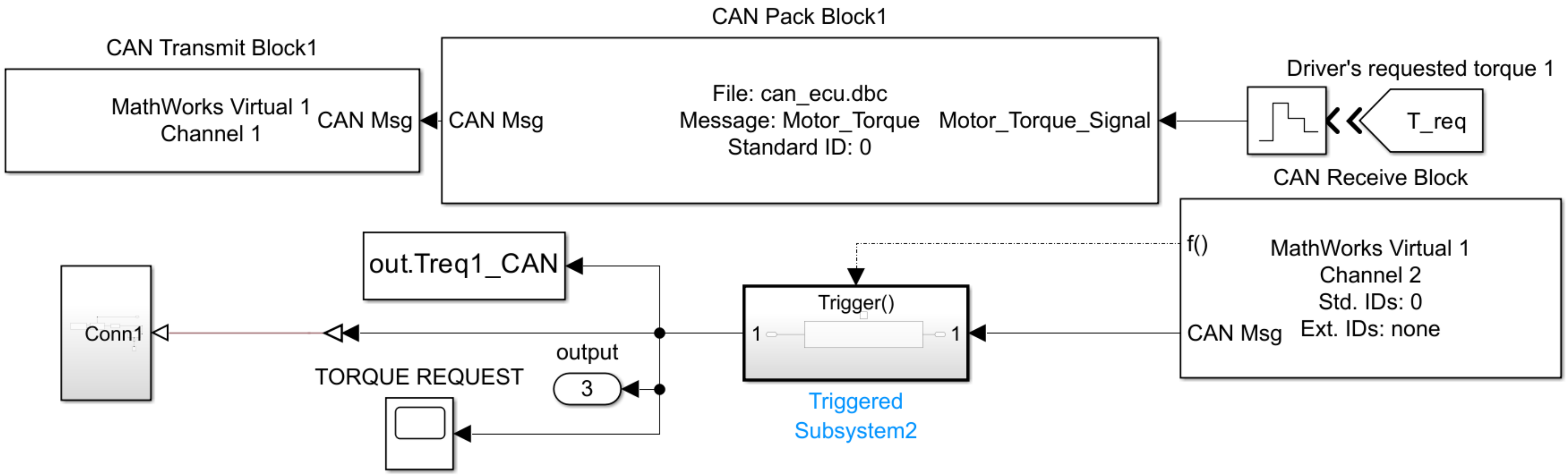
INTEGRATED CAN BUS MODEL

VECTOR >

CANdb++

CANdb++ Editor essential for designing and editing CAN databases

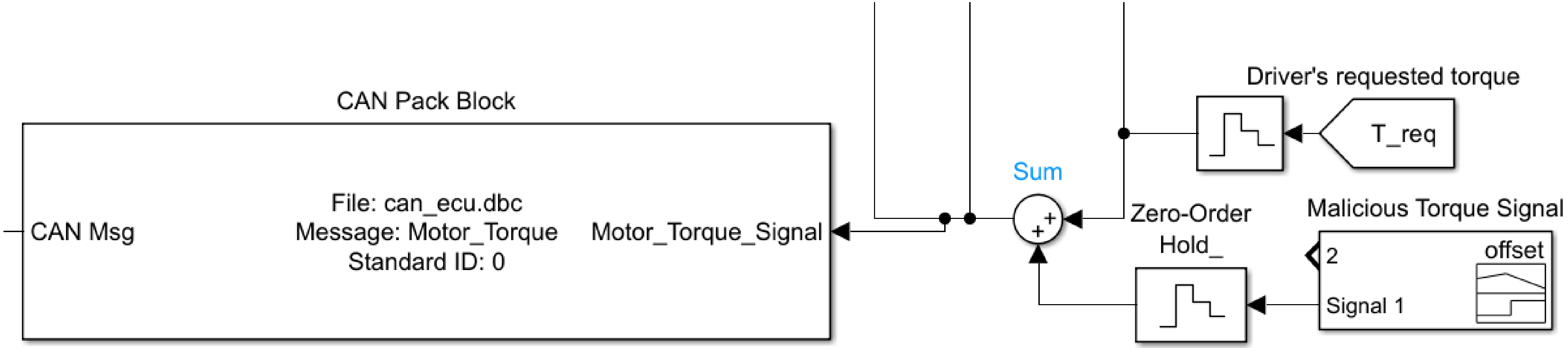
- Simulate regular and malicious network behaviors
- Generate CAN DataBase (DBC) file



CAN BUS INJECTOR MODULE

Simulink signal builder block:

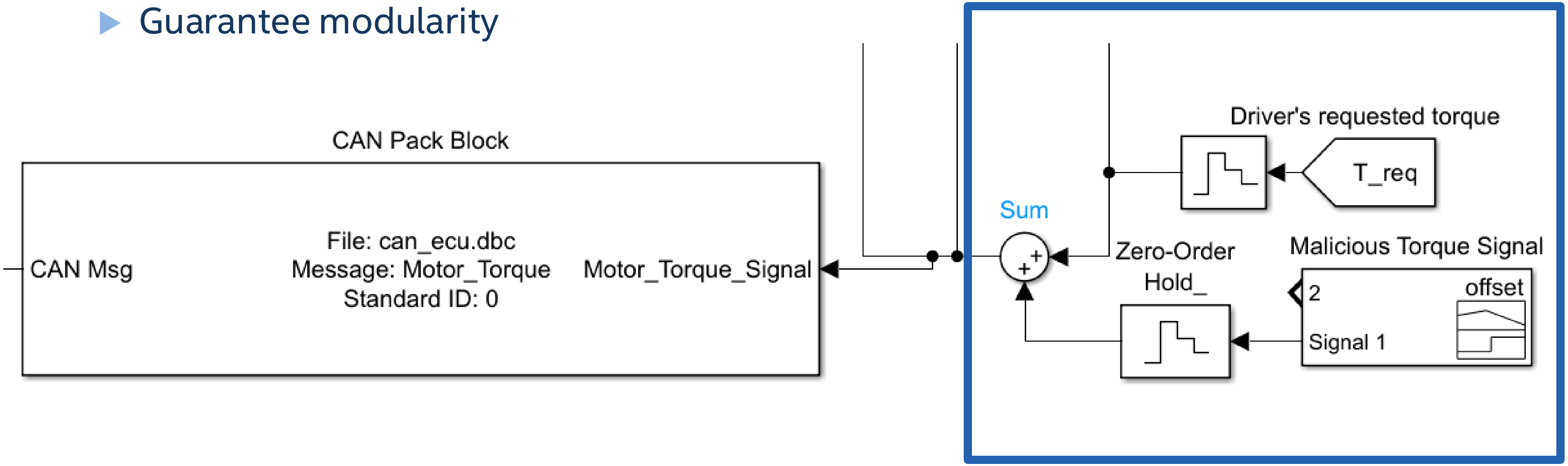
- Build various attack signals
- Simulate multiple attack scenarios



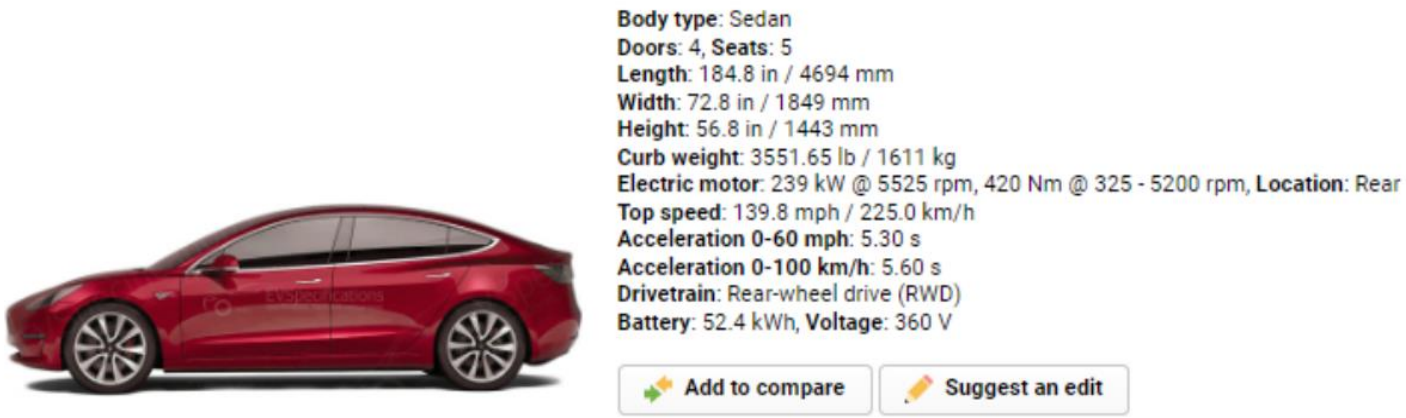
CAN BUS INJECTOR MODULE

Summing block

- Can be programmed separately
- Leaving the original model unaltered
- Guarantee modularity



EXPERIMENTAL SET UP

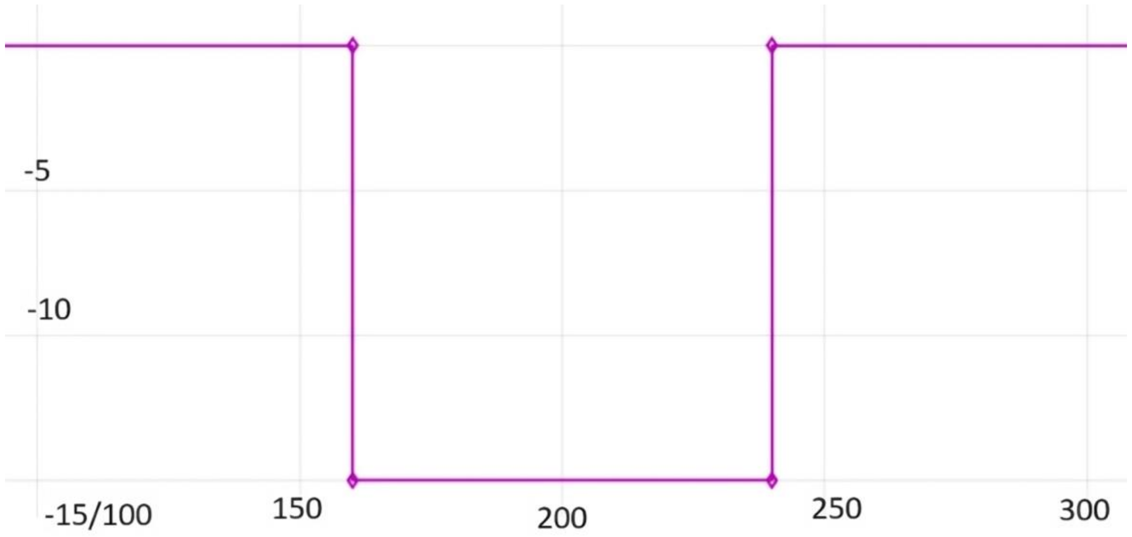


Body type: Sedan
Doors: 4, **Seats**: 5
Length: 184.8 in / 4694 mm
Width: 72.8 in / 1849 mm
Height: 56.8 in / 1443 mm
Curb weight: 3551.65 lb / 1611 kg
Electric motor: 239 kW @ 5525 rpm, 420 Nm @ 325 - 5200 rpm, **Location**: Rear
Top speed: 139.8 mph / 225.0 km/h
Acceleration 0-60 mph: 5.30 s
Acceleration 0-100 km/h: 5.60 s
Drivetrain: Rear-wheel drive (RWD)
Battery: 52.4 kWh, **Voltage**: 360 V

- Tesla model 3
- 2 scenarios:
  - Extra Urban Driving Cycle
  - Cruise mode

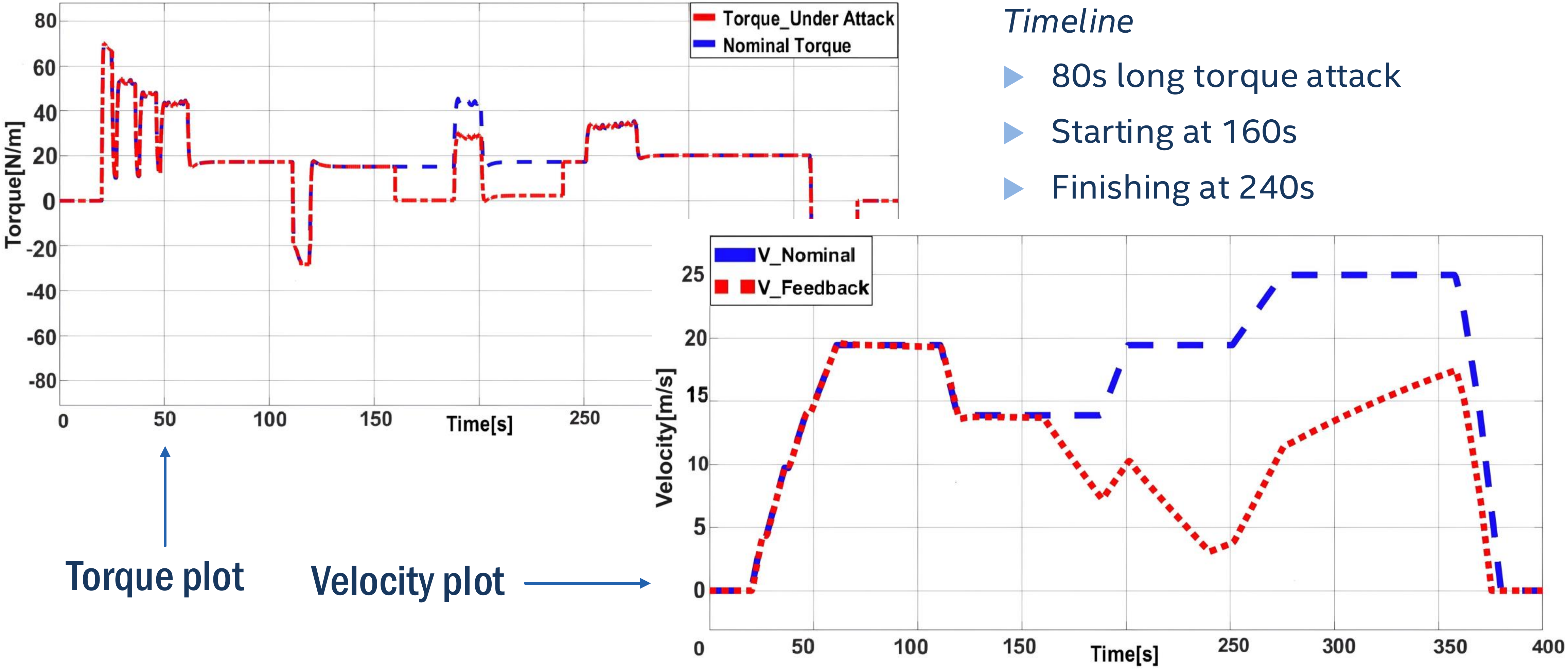
Injected torque signal:

- Step signal amplitude = −15Nm
- Between t = 160s and t = 240s
- Altering velocity



Does the model react correctly?

EXTRA URBAN DRIVING CYCLE



Torque plot

Velocity plot

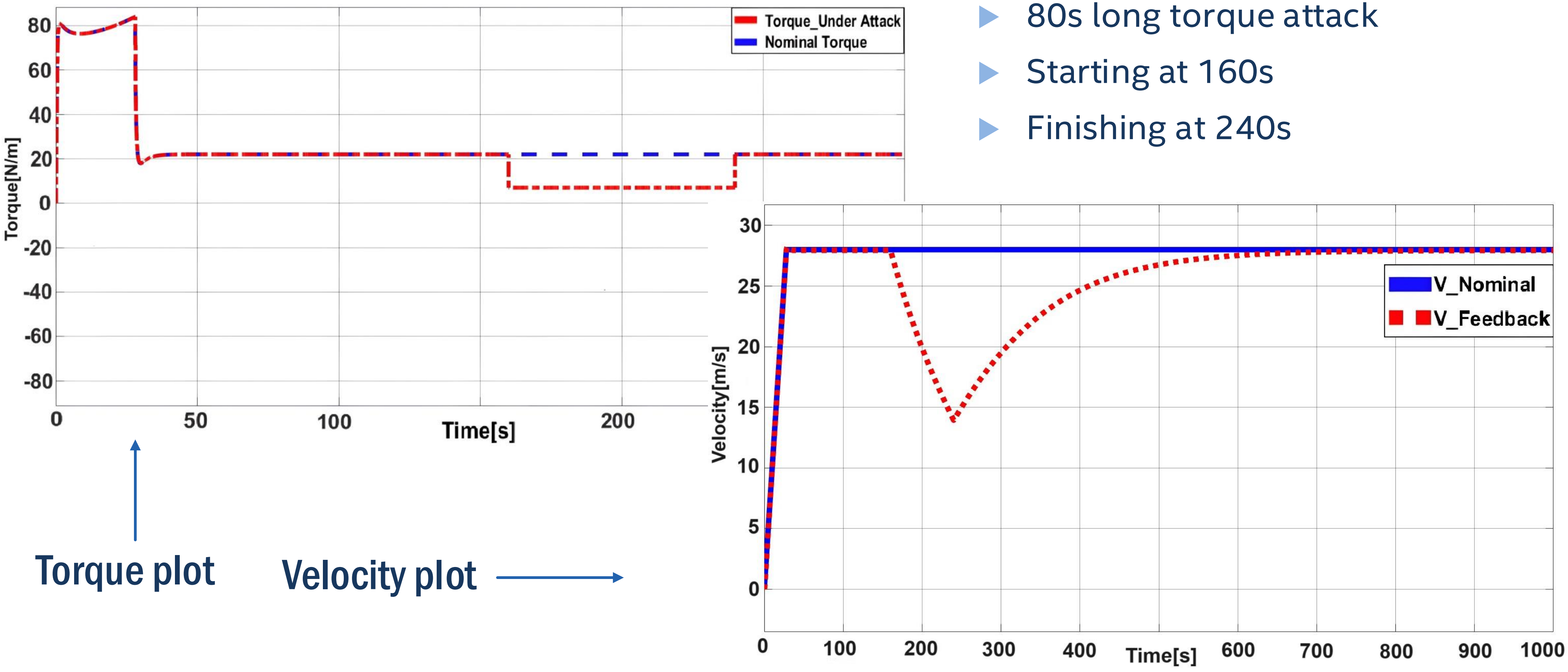
Timeline

- 80s long torque attack
- Starting at 160s
- Finishing at 240s

CRUISE MODE

Timeline

- 80s long torque attack
- Starting at 160s
- Finishing at 240s



Torque plot

Velocity plot

CONCLUSION AND FURURE WORK

Contributions:

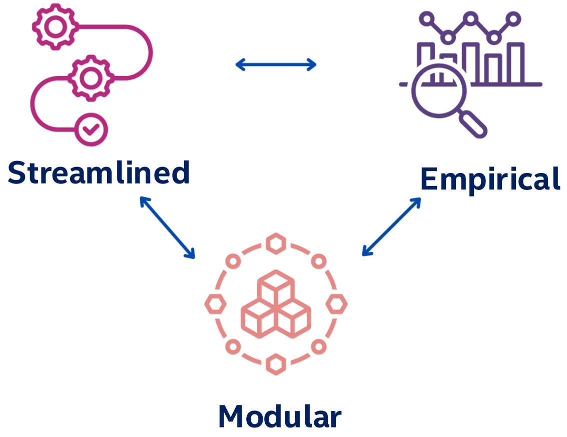
- 3-component modular architecture
- Easy to collect CAN data changing vehicles and attacks
- Analyze the effect on the vehicle dynamics
- Use case: Tesla model 3, torque attack, 2 driving scenarios

The implementation has been released on GitHub

https://github.com/smilies-polito/CARACAS

Future work

- Validate the system comparing the generated data with real world data
- Design and collect a dataset of attacks using this framework
- Exploit the dataset to train IDSs



SMILIES
reSilient coMputer archItectures
and LIfE Sciences

Politecnico
di Torino

Department of Control and
Computer Engineering

DAUIN

Thanks for your kind attention!

Any questions?

LinkedIn

Nicola Scarano
nicola.scarano@polito.it
Ph.D. student

SMILIES research group
Department of Control and Computer Engineering
Politecnico di Torino, Turin, Italy

LICENSE