Eclipse KUKSA.val for SCR Anti-Tampering Monitoring in Heavy Vehicles

Junhyung Ki[*], Sebastian Schildt[Δ], Andreas Hastall[Δ], Sven Erik Jeroschewski[▪], Robert Höttger[*/◊]

[*] Dortmund University of Applied Sciences and Arts / [Δ] Robert Bosch GmbH / [▪] Bosch.IO GmbH / [◊] Materna Information & Communications SE

This work was funded by the European Union's Horizon 2020 Research and Innovation Programme through DIAS project (https://diasproject.com/) under Grant Agreement No. 814951.

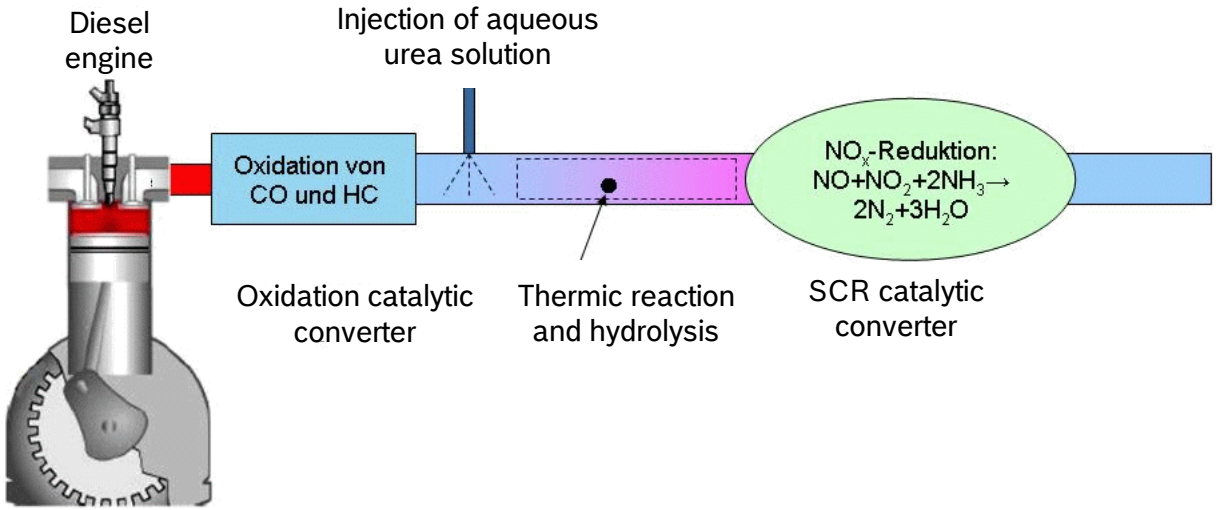
THE PROBLEM

DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS

Introduction
Diesel Exhaust Treatment

- Diesel Engines use “Selective Catalytic Reduction” (SCR) as part of the exhaust treatment system
- The SCR system converts harmful nitrogen oxides (NO_x) from the exhaust gas into Nitrogen ($N_{2)}$ and Water (H_20)
- This reaction requires ammonia (NH_3) that needs to be fed to the system. This is usually done in form of a urea solution (marketing name “AdBlue”)
- Required to meet legislated emission standards

For more technical details check:
https://dieselnet.com/tech/cat_scr_diesel_urea_dosing.php



AdBlue Tankeinfuellstutzen by Kickaffe under CC BY-SA
SCR schematic by Hastdutoene under CC BY-SA

The Danger
Tampering

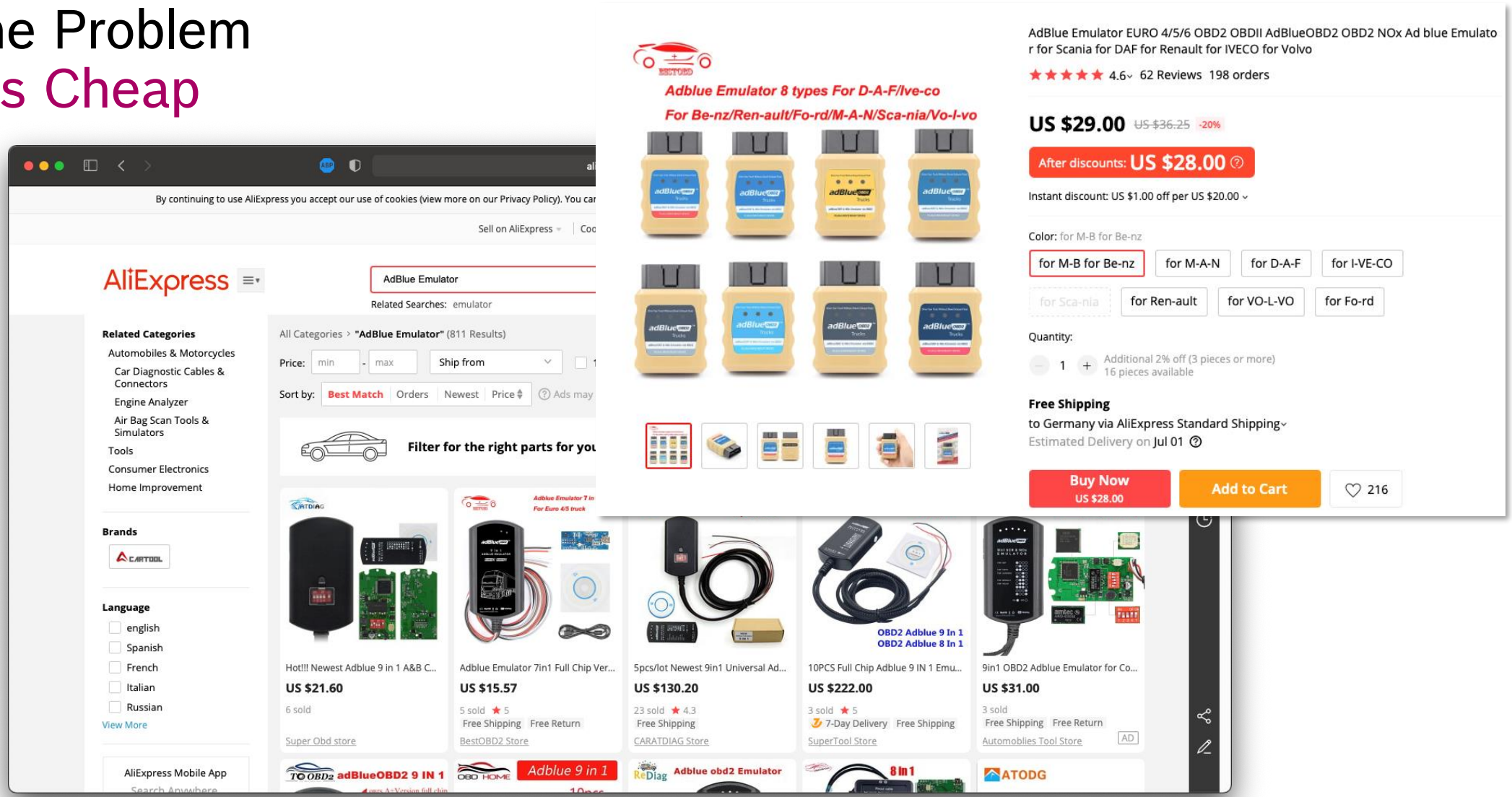
- AdBlue is a cost factor: It can add 1500USD/year operating cost to a commercial vehicle
- Without AdBlue a legally compliant truck will not start

The cost provides an incentive to ***tamper*** with the system

- Deactivating parts of the SCR systems and related sensors
- Sending fake data on vehicle busses to prevent the on-board systems to detect it
- This is nearly impossible/time consuming to detect by traffic police

Esso AdBlue pump by Cjp24 under CC BY-SA

The Problem
It is Cheap



WORKING ON A SOLUTION

DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS

DIAS Project
Diagnostic Anti-Tampering Systems

Malicious tampering of environmental protection systems like SCR turns very clean vehicles in heavy polluters. In the European project DIAS, countermeasures are developed to harden vehicles against tampering.
11 partners from 7 countries.

A thorough two-level plan to stamp out tampering
DIAS starts with current OBD and follows a two-level approach. The first level is the development of an enhanced OBD system, assessing its resistance to tampering and creating intermediate regulatory guidelines. The second level will be the development of more advanced cloud-based diagnostics systems involving two-way communication that foresees swift tampering detection.

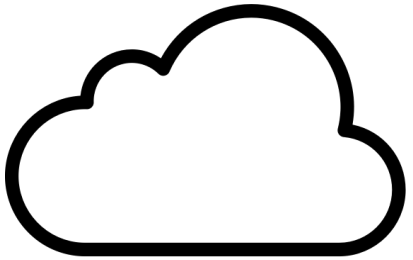
https://www.dias-project.com

Eclipse KUKSA
Software Components for Connected Vehicles

“The open Eclipse KUKSA project aims to provide standardized software building blocks for connected car ecosystems that can be shared across the industry, providing performance, quality and scalability for base services that can act a solid foundation for a variety of competing products and services.”

In-vehicle components

- KUKSA.val V(I)SS dataserver
- KUKSA.hardware



KUKSA.cloud

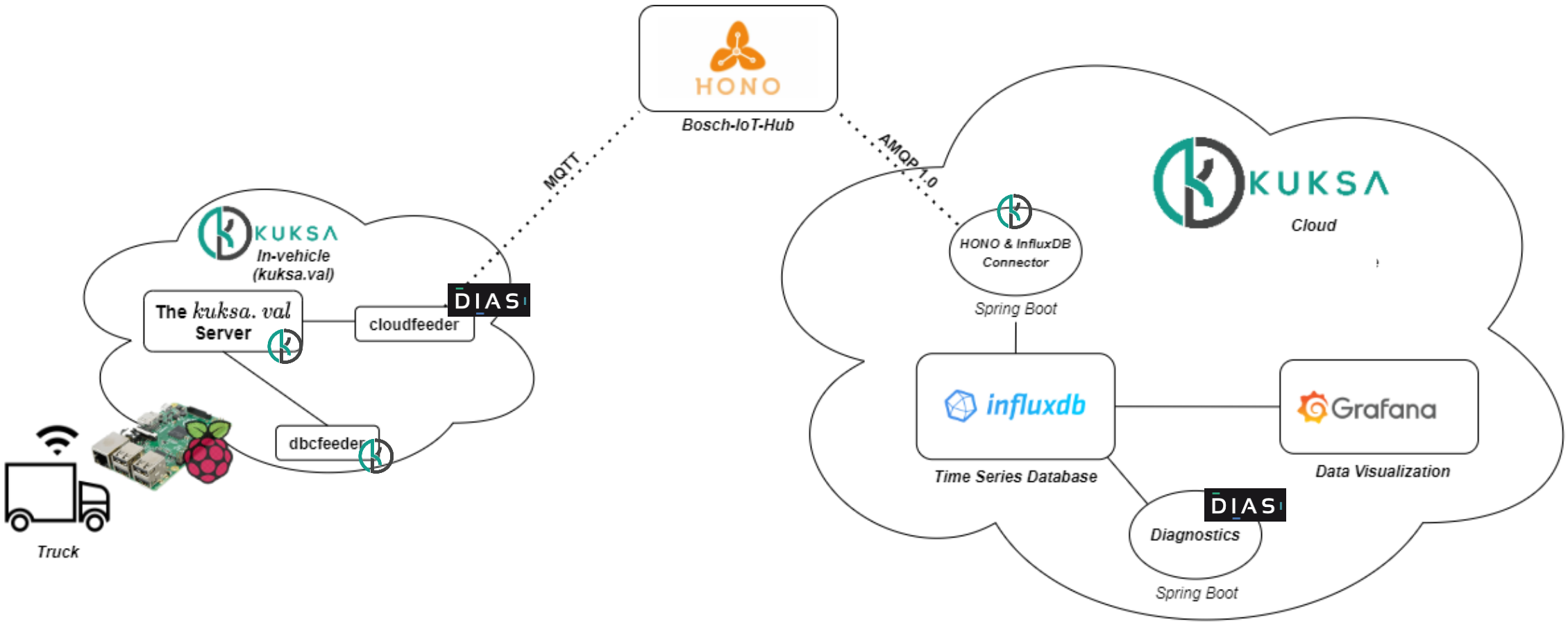
- Distribution of services for connected vehicles
- Relying on Eclipse IoT technologies

https://www.eclipse.org/kuksa/

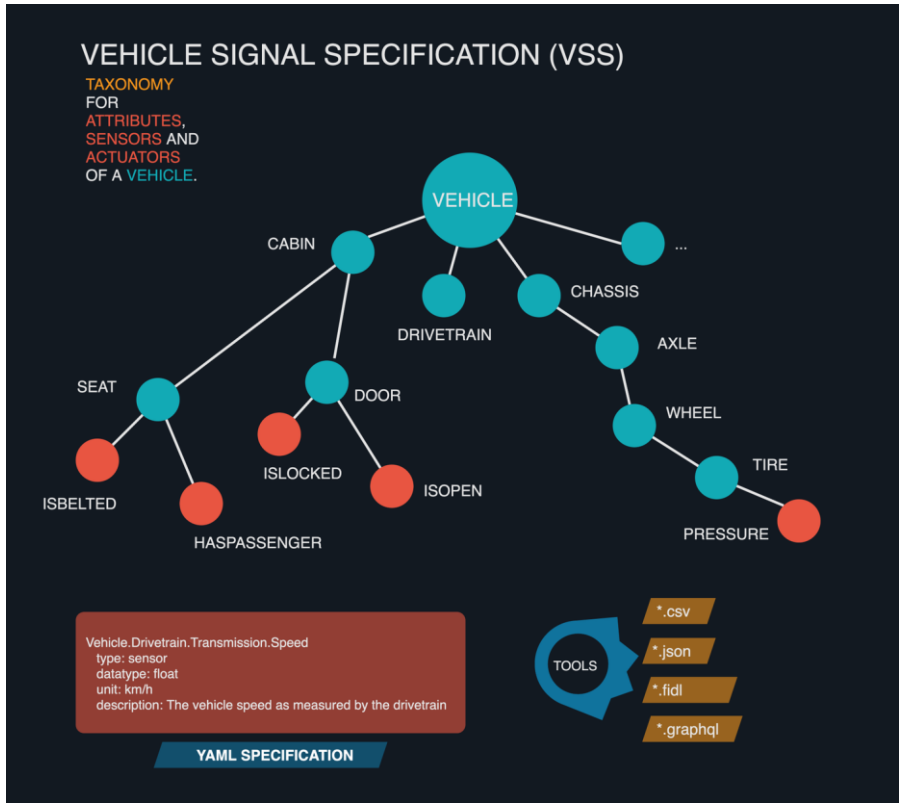
OUR APPROACH

DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS

SCR Anti-Tampering with KUKSA
System Overview



SCR Anti-Tampering with KUKSA
Genivi Vehicle Signal Specification



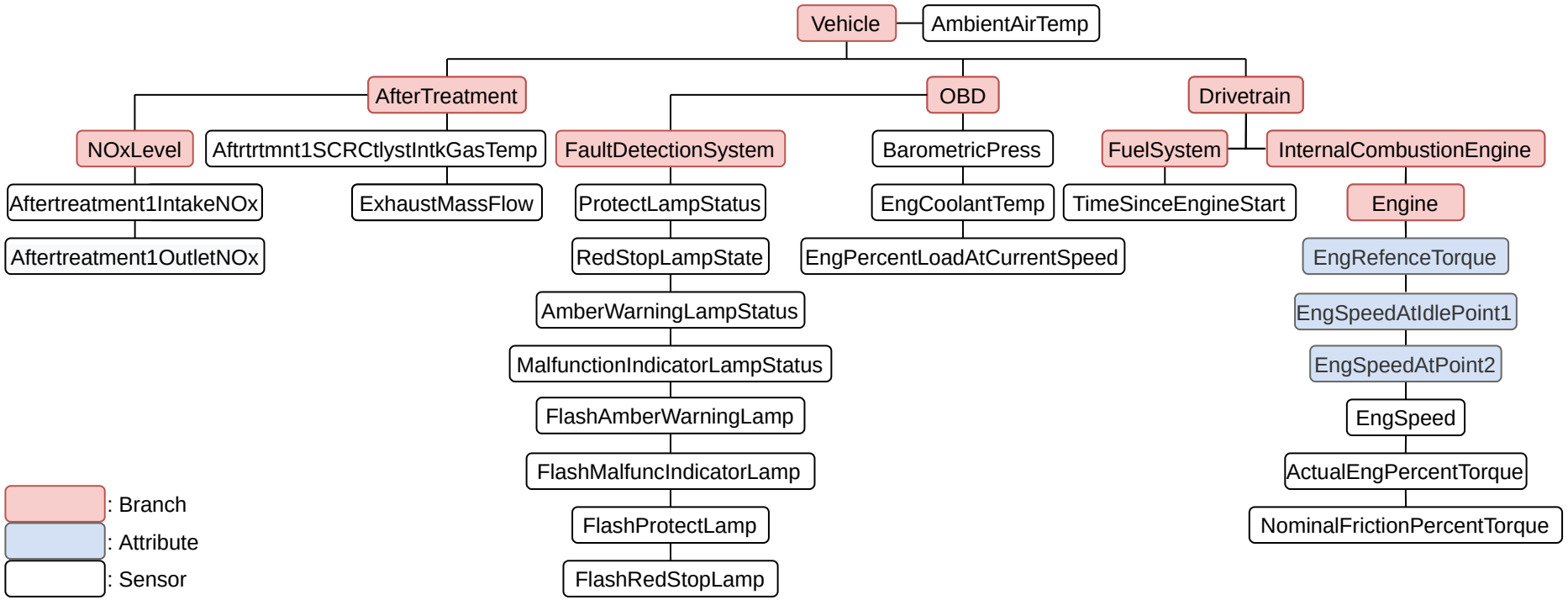
- Introduces a domain taxonomy for vehicle signals
- Creating a common understanding of vehicle signals in order to reach a “common language” for vehicle data independent of protocol or serialization format.
- Cooperatively created by various industry players
- Completely open

Example: Vehicle.Powertrain.Battery.Temperature

```
"Temperature": {
"datatype": "float",
"description": "Temperature of the battery pack",
"type": "sensor",
"unit": "celsius",
"uuid": "2b9d90f1d87c57dcbbd6a72807f8d412"
}
```

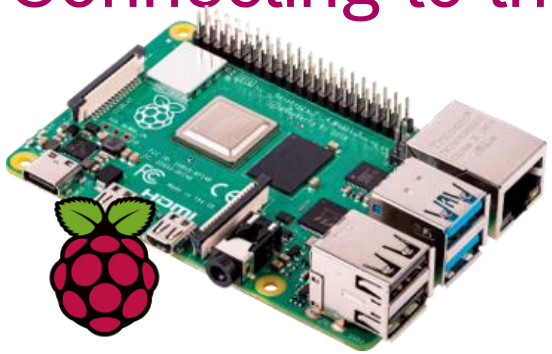
https://github.com/genivi/vehicle_signal_specification

SCR Anti-Tampering with KUKSA
VSS Model for Anti-Tampering Prototype

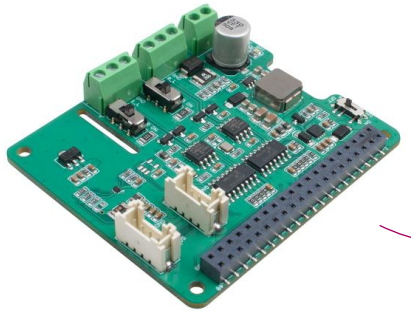


SCR Anti-Tampering with KUKSA

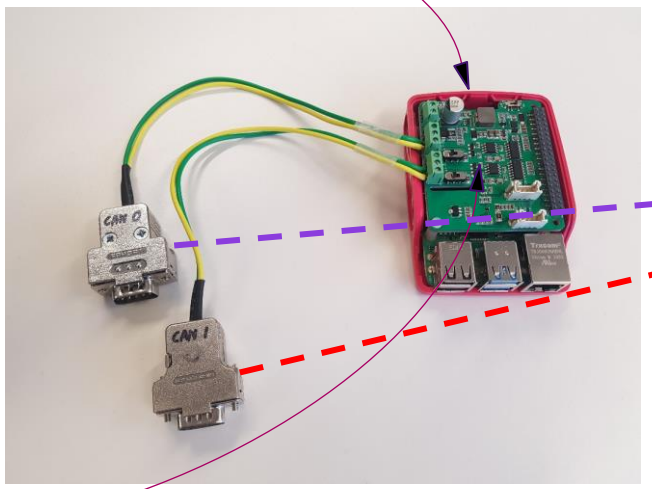
Connecting to the vehicle in our experiment



Raspberry Pi 4



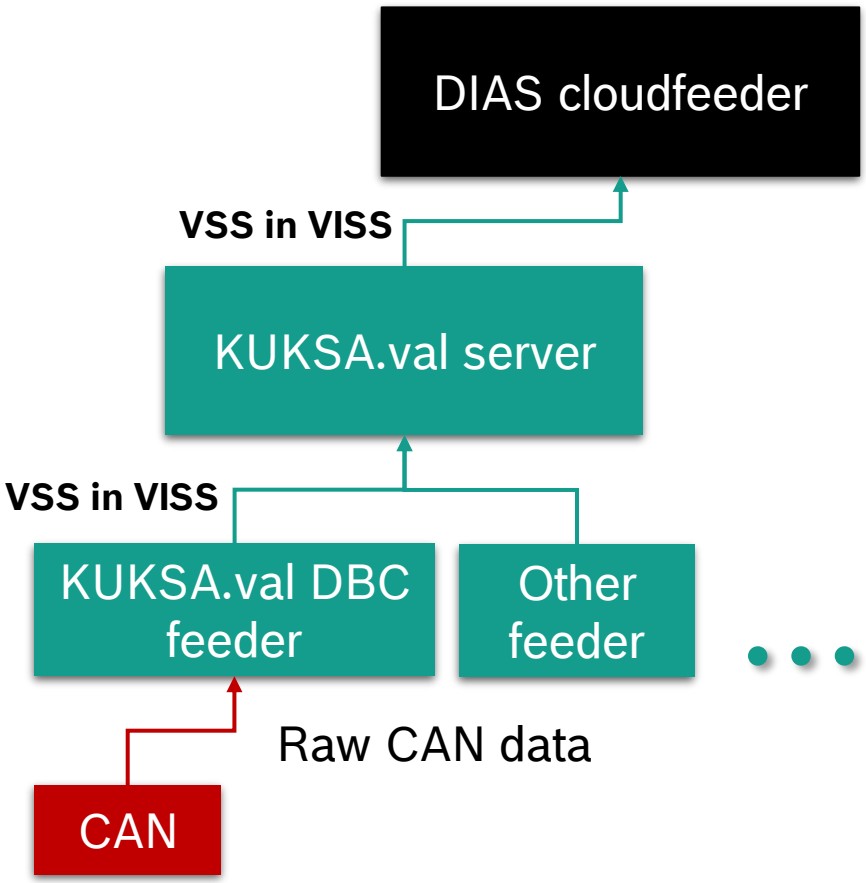
2-Channel CAN Shield
(Seeed Studio)



Truck
ECU

Two CAN channels are used here because modern vehicles have several independent CAN busses and in our test vehicle the relevant signals are spread across two CAN busses

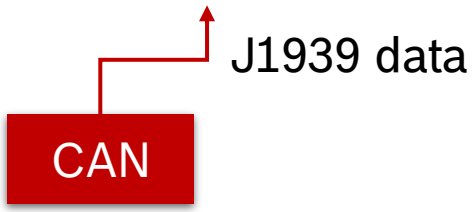
SCR Anti-Tampering with KUKSA
Accessing signals with KUKSA.val



- Proprieatary frames are read from CAN
- A KUKSA *feeder* component transforms them into a format described using the standardized Genivi VSS (Vehicle Signal Specification)
- The VSS datapoints are then transferred to the KUKSA.val server using the standardized W3C VISS (Vehicle Information Service Specification) protocl
- Applications can access the data via VISS

SCR Anti-Tampering with KUKSA
J1939 extension for KUKSA.val DBC Feeder (1)

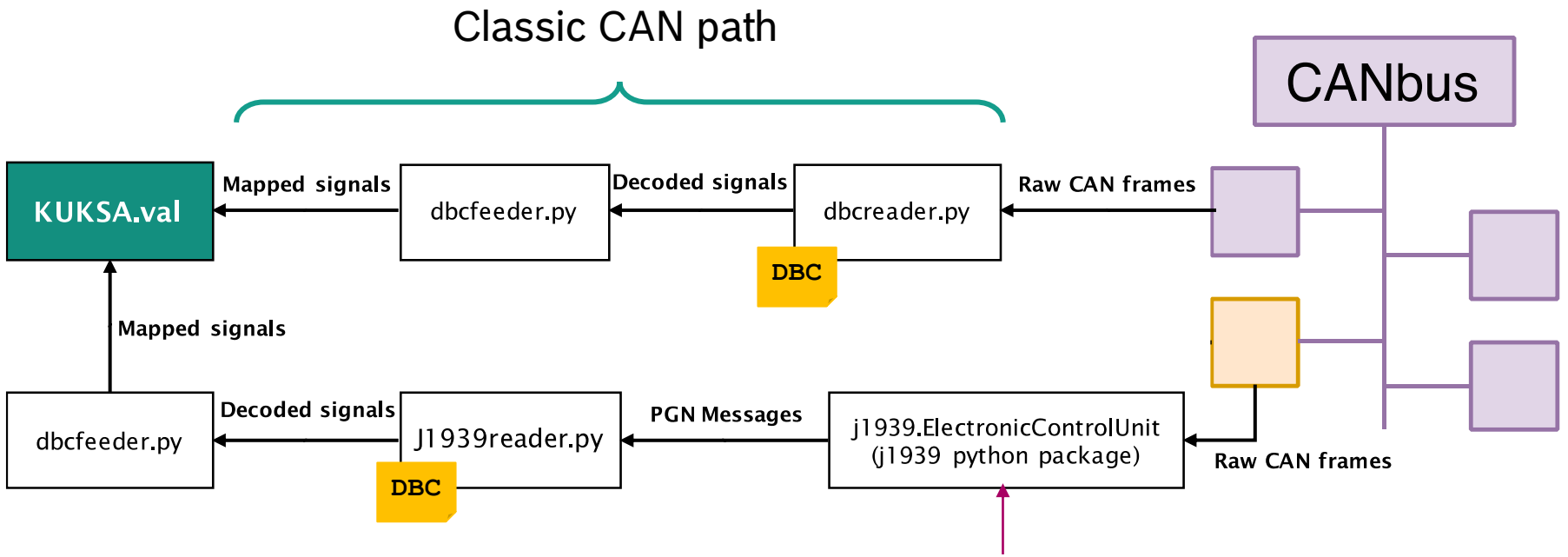
- When starting, KUKSA.vals DBC feeder just supported raw CAN frames, as are commonly used in passenger vehicles
- Heavy duty vehicles such as trucks often use SAE-J1939
  - J1939 is still using CAN for transport
  - It adds a higher layer protocol, that – among other things – supports logic data frames larger than one CAN frame (8 bytes for classic CAN)
  - Signal locations based on “PGN” (Parameter Group Number) instead of CAN ID
  - Can be described in a DBC File



https://www.sae.org/standardsdev/groundvehicle/j1939a.htm
https://www.csselectronics.com/screen/page/simple-intro-j1939-explained/language/en#j1939-pgn-spn

SCR Anti-Tampering with KUKSA

J1939 extension for KUKSA.val DBC Feeder (2)

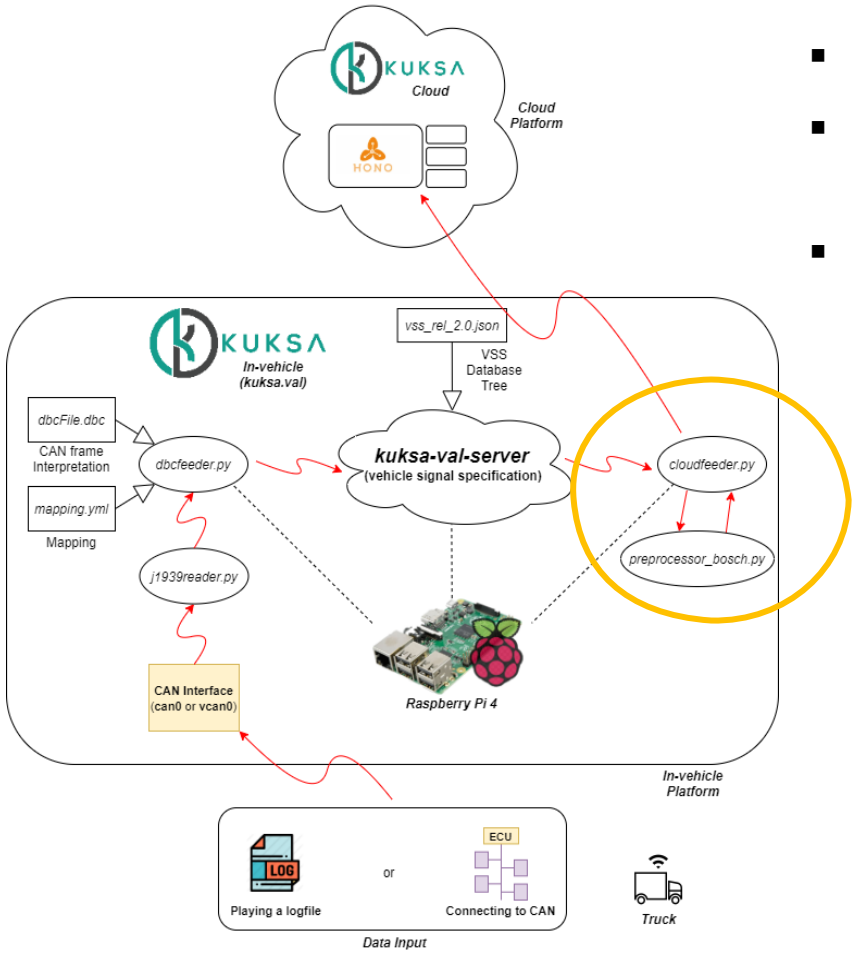


This has been contributed to KUKSA.val by the DIAS project and has been merged.

Everybody can use it now

https://github.com/eclipse/kuksa.val/tree/master/kuksa_feeders/dbc2val

SCR Anti-Tampering with KUKSA
DIAS Cloud feeder



- Fetches required signals from *KUKSA.val server*
- *P*re-processes the fetched signals' values with variable preprocessor script
- Sends the pre-processed result as telemetry data to the cloud via MQTT

Fetched signals

Pre-processed result telemetry

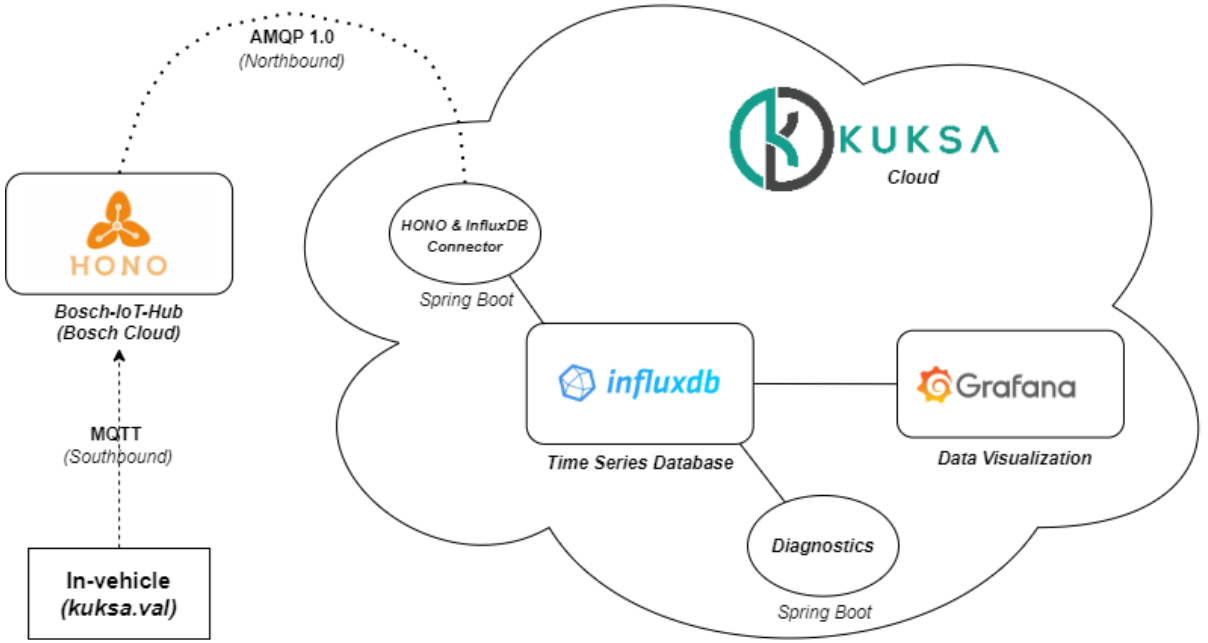
MQTT transmission

```
junh-ki@junhki-VirtualBox: ~/Desktop/kuksa.val/clients/vss-testclient
File  Edit  View  Search  Terminal  Help
######################## Signals ########################
AftrtrtmntSCRCtlystIntkGasTemp :  220
Aftertreatment1IntakeNOx :  341.3999938964844
Aftertreatment1OutletNOx :  0
AftrtratmentExhaustGasMassFlow :  685.0
NominalFrictionPercentTorque :  6.0
AmbientAirTemp :  1.875
BarometricPress :  98.0
EngCoolantTemp :  84.0
EngPercentLoadAtCurrentSpeed :  75.0
EngReferenceTorque :  2705.0
EngSpeedAtPoint2 :  1800.0
EngSpeedAtIdlePoint1 :  550.0
EngSpeed :  1190.5
ActualEngPercentTorque :  52.0
TimeSinceEngineStart :  181
MalfunctionIndicatorLampStatus :  0
######################## Telemetry ########################
Telemetry: {'sampling_time': {'total_sampling': 17, 'tscr_bad': 1, 'tscr_intermediate': 0, '
tscr_good': 16, 'old_good': 0, 'pems_cold': 0, 'pems_hot': 16}, 'tscr_good': {'11': {'cumula
tiveNOxDS_g': 0.0, 'cumulativeNOxDS_ppm': 0, 'cumulativeNOxUS_g': 0.5005722954932131, 'cumul
ativeNOxUS_ppm': 1655.2999877929688, 'cumulativePower_J': 787976.3873304392, 'cumulativePowe
r_kWh': 0.21888232981401085, 'samplingTime': 5}}, 'pems_hot': {'11': {'cumulativeNOxDS_g': 0
.0, 'cumulativePower_J': 787976.3873304392, 'cumulativePower_kWh': 0.2188823298140108, 'sam
plingTime': 5}}}

# Socket Connected :)
# Current telemetry being sent...
Client mosqpub|13496-junhki-Vi sending CONNECT
Client mosqpub|13496-junhki-Vi received CONNACK
Client mosqpub|13496-junhki-Vi sending PUBLISH (d0, q0, r0, m1, 'telemetry', ... (557 bytes)
)
Client mosqpub|13496-junhki-Vi sending DISCONNECT
# Successfully done!
```

https://github.com/junh-ki/dias_kuksa/

SCR Anti-Tampering with KUKSA
KUKSA.cloud setup



* AMQP (Advanced Message Queue Protocol)
* MQTT (Message Queuing Telemetry Transport)

Bosch-IoT-Hub (Eclipse Hono)

- Remote service interfaces for connecting IoT devices in a uniform way

Hono-InfluxDB-Connector

Connects to Hono and InfluxDB, to receive and store data

InfluxDB

- Data are stored in chronological order

Grafana

- Visualizes data in InfluxDB

Diagnostics

- Evaluates data in InfluxDB

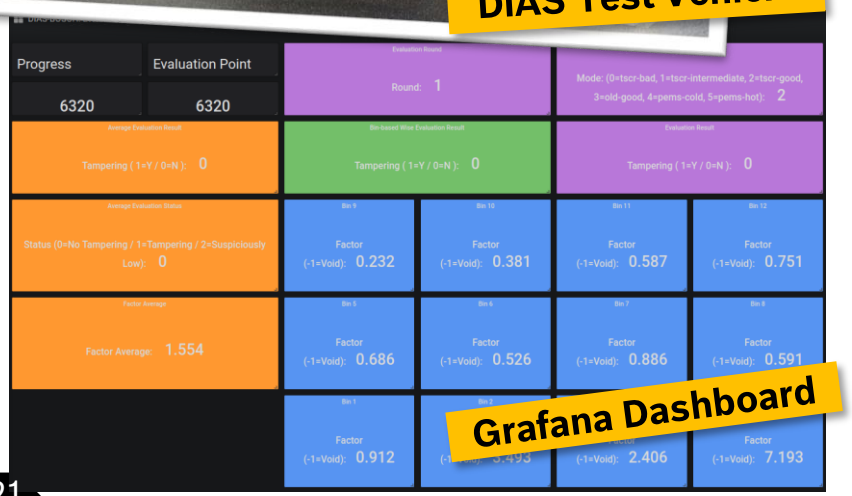
PUTTING IT ALL TOGETHER & FINAL THOUGHTS

DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS

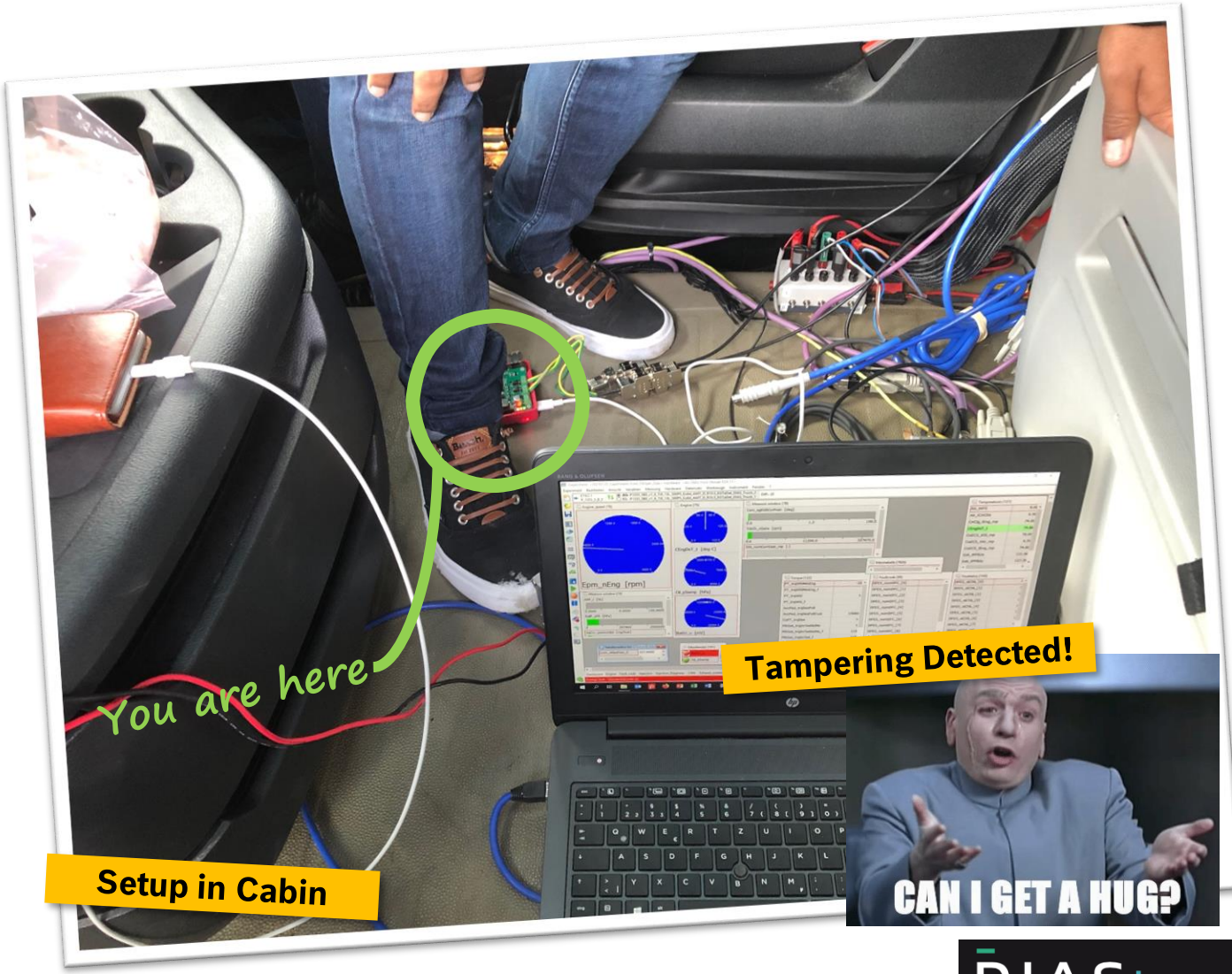
SCR Anti-Tampering with KUKSA

Testing…

DIAS Test Vehicle



Grafana Dashboard



Setup in Cabin

SCR Anti-Tampering with KUKSA
Open points and future work

- “Deepen” security:
  - Currently we need to “trust” data received from CAN bus, and detect tampering solely through inconsistency, plausibilisation
  - Mechanisms for authenticating data on CAN exist, but are not widely deployed yet. Would be a good first line of defence
- Limits of OSS approach
  - The proposed system, tested on a Pi can easily run on a modern (processor-based) Vehicle Computers. However, requires modern vehicles that offer suitable runtimes/sandboxes for modern software
  - The “deeper” you go, the more proprietary vehicle architectures get. Probably there will not be much OSS/open systems in the layers below Vehicle Computers
- Not all data used for this use case is specified in the standard VSS data catalogue (yet)

SCR Anti-Tampering with KUKSA
Learnings

- Building DIAS SCR Anti-Tampering system starting **from a vehicle bus to the cloud** is possible using only **Open Source** technologies
- Adapting existing solutions is much faster than starting from scratch for “non-core” topics such as
  - In-vehicle data server
  - Connectivity
  - Cloud infrastructure
- Some assembly required: Provided initial J1939 support back to Eclipse KUKSA, saving more time on the next use case
- No need to share application IP (detailed algorithm for detection) when using Eclipse KUKSA:

“Open base services as a solid foundation for a variety of competing products and services”

DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS

https://www.dias-project.com

KUKSA

https://www.eclipse.org/kuksa/

BOSCH

Andreas Hastall

Powertrain Solutions
Advanced Engineering
Engineering Legislation and OBD System

Robert Bosch GmbH,
Robert-Bosch-Platz 1
70839 Gerlingen-Schillerhöhe

andreas.hastall@de.bosch.com

https://www.bosch-mobility-solutions.com/

BOSCH

Dr.-Ing.
Sebastian Schildt

Corporate Sector Research and
Advanced Engineering
Communication and Network Technologies

Robert Bosch GmbH,
Robert-Bosch-Campus 1
71272 Renningen

sebastian.schildt@de.bosch.com

https://www.bosch.com/research/

QUESTIONS?

DIAS
DIAGNOSTIC ANTI-TAMPERING SYSTEMS