DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

DIAS overview

25th October 2022, Brussels

HORIZON 2020
LC-MG-1-4-2018
Grant agreement ID: 814951

DIAS
Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION
HORIZON 2020
LC-MG-1-4-2018
Grant agreement ID: 814951

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814951.

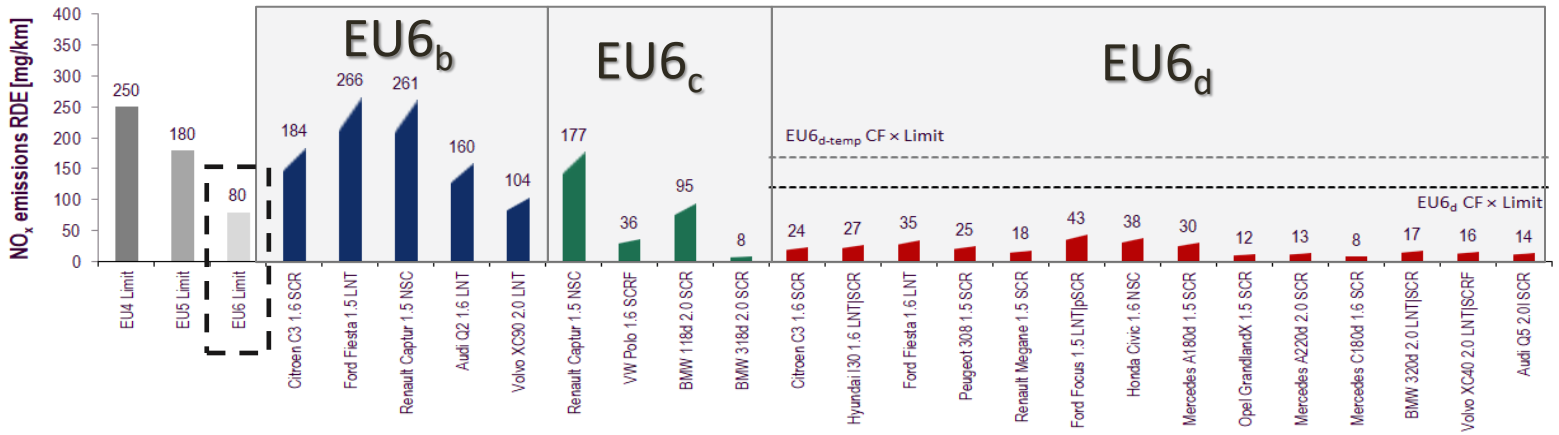
The DIAS consortium

- Smart Adaptive Remote **Di**agnostic **A**ntitampering **S**ystems
- 11 partners with various competencies
- Part of H2020 European programme (smart, green and integrated transport sector)
- International co-operation
- Budget: €4.99M
- Duration: 38 months (Sept. 2019 – Oct. 2022)

DIAS

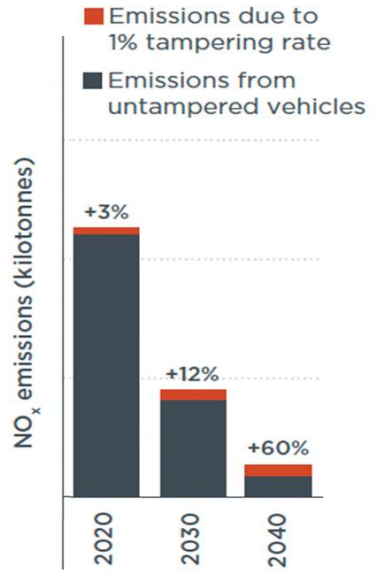
Problem statement

- NOx emissions (diesel):
  - EU6d fleet average: 20-30 mg/km thanks to the development of effective Environmental Protection Systems (EPS)
  - Tampered vehicle: More than x10 higher emissions



Tampered Vehicles

- Even a small percentage of tampered vehicles (1%) can lead to a huge increase in fleet emissions in the future (+60% for 2040)
- **Up to 10% of EU5/V and EU6/VI vehicles** in the EU are estimated to have been **tampered** with their environmental protection systems



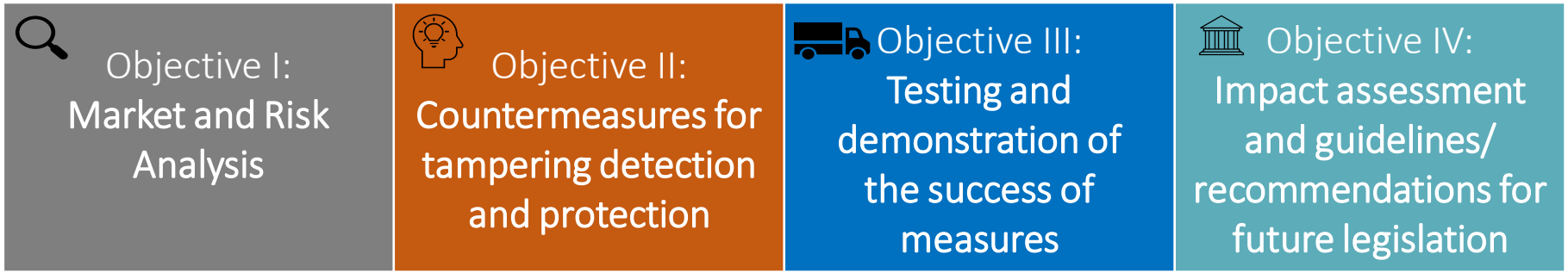
DIAS

Objectives of DIAS

1. **Detect tampering** using On-Board Diagnostics and Monitoring (OBD/OBM)
2. **Prevent tampering** via hardened in-vehicle communication and component security
3. **Report** tampering events and relevant data to appropriate authorities

Target: Make tampering **economically unattractive and reduce emissions**

Our methodology:



DIAS

Overview of market and risk analysis

Initial inputs:

- Security analysis
- Tampering Practices
  Tampering Devices/Market Assessment
- Testing

Specifications of countermeasures to be developed:

- ❑ Environmental Protection Systems (EPS) to be covered:
  - DeNOx
  - DPF
  - TWC
  - GPF
- ❑ Components to be covered:
  - ECU
  - CAN
  - Sensors
  - …
- ❑ Tampering methods to be covered:
  - ECU reflashing
  - Emulators
  - Modifiers
  - DTC erasers
- ❑ Vulnerabilities to be covered:
  - Simulated signal
  - Clear DTCs
  - Change ECU maps
  - Hardware access
  - …
- ❑ Categories of solutions to be covered:
  - Diagnostic
  - Security
  - Reporting

Overview of identified solutions

- **Diagnostic solutions:**
  - **Monitoring and plausibilisation of signals**
    - Diagnosis of DPF/GPF-related attacks
    - Diagnosis of deNOx (EGR & SCR)-related attacks
    - Diagnosis of TWC-related attacks
    - Diagnosis of all-EAS-related attacks
  - **Estimation of tampering probability**
    - Diagnosis of all-EAT-related attacks

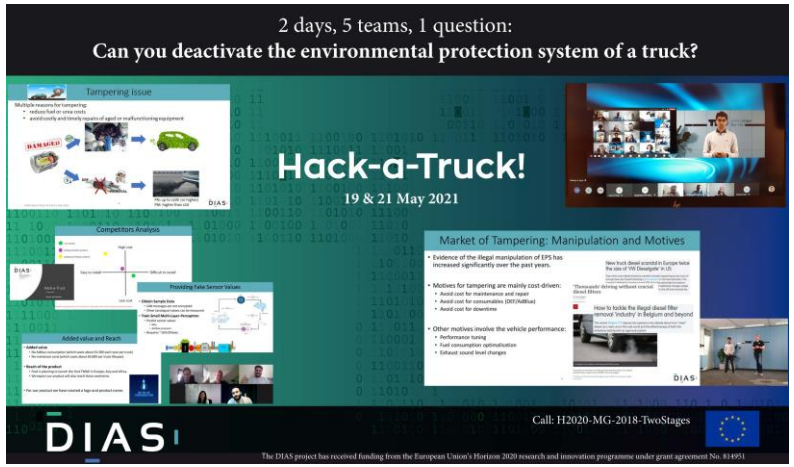
- **Security solutions:**
  - **Component Security**
    - Boot Security
    - Firmware Update Security
    - Prevent the exploitation of memory corruption vulnerabilities
  - **Communications Security**
    - Key generation, exchange and storage
    - Data exchange authentication, integrity and encryption
  - **Intrusion Detection and Firewall**
    - Intrusion Detection System
    - Firewall

- **Reporting solutions:**
  - **Reporting scheme**
    - Generic scheme of tampering-related data reporting
    - NOx emissions related data aggregation, preprocessing, storage and transfer rate
  - **Reporting infrastructure**
    - In-vehicle data aggregation/preprocessing and transfer to cloud
    - On-cloud data aggregation/preprocessing and transfer to reporting authorities
  - **Emissions compliance certification**
    - Final tampering report (certificate)

Overview of conducted demonstrations

- Installation of anti-tampering systems on demonstrators:
  - Demonstrator vehicle provided by partner Ford OTOSAN
  - Stand-alone lab demonstrators

- Evaluation of anti-tampering systems via:
  - **Internal** verification and validation of the system
  - **External** hacking events:
    - Analysis of vehicle hardware and software by IT security experts and hackers
    - Hackathon #1 organized in May 2021
    - Hackathon #2 organized in March 2022



→ Received feedback led to adjustments on DIAS solutions and further considerations

Overview of future regulatory framework

Guidelines for various end-users

- **Vehicle manufacturers:** Provide vehicle's anti-tampering solutions for tampering prevention, detection and reporting for and after the Type Approval

- **Type Approval authorities**: Ensure that the anti-tampering provisions addressed to vehicle manufacturers are met

- **Member States:** Transpose into national law and enforce tampering-related EU regulatory framework

- **Other authorities** (i.e. Periodic Technical Inspection, Roadside Inspection): Identify high emitters and tampered vehicles and report tampering

- **Workshops**: Ensure legitimate use of diagnostic tools and report tampering

- **Vehicle owners**: Ensure proper and timely maintenance and proper "reverting" actions if tampering is concluded

DIAS

Overview of impact assessment results

- Over the 2022-2050 period, the maximum theoretical benefits that can be achieved in an ideal case where 100% of the tampering is eliminated, and based on the most **realistic estimations** for tampering inputs*:
  - **3.7** megatonnes savings on NOx emissions
  - **41** kilotonnes savings on PM emissions
  - **26,000** avoided premature deaths
  - **460,000** avoided years of life lost
- **Half benefit** based on most **optimistic estimations** for tampering inputs
- **Double or triple benefit** based on **worst-case estimations** for tampering inputs (e.g. 81,000 premature deaths can be avoided)

*i.e. The share (in %) of tampered vehicle in the European fleet and the ratio of tampered to non-tampered vehicle emissions

DIAS

DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Thank you

Q & A

DIAS
SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS