Tampering of Emission Controls and Countermeasures

Dimitrios Kontses, Zissis Samaras

Laboratory of Applied Thermodynamics
Aristotle University of Thessaloniki, Greece

Contributions from DIAS project

Many thanks to the Work Package leaders:

- Ann Delahaye (TNO)
- Miao Zhang (FEV)
- Andreas Hastall (Bosch)

and all other DIAS colleagues

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

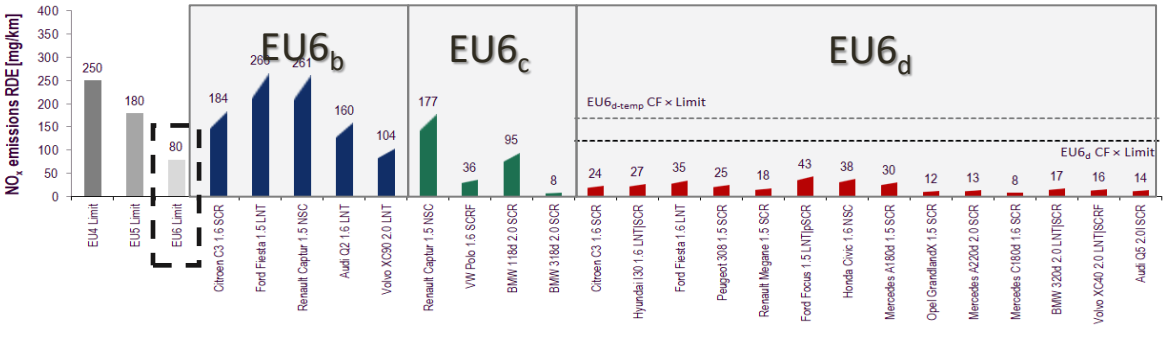
Disclaimer: *This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains*

Introduction-The DIAS consortium

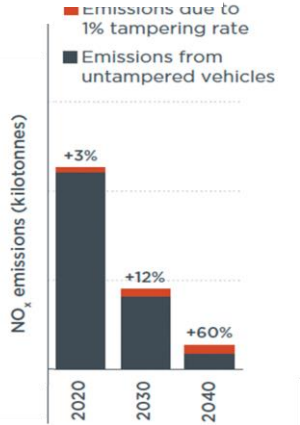
- Smart Adaptive Remote **Di**agnostic **A**ntitampering **S**ystems
- 11 partners with various competencies
- Part of H2020 European programme (smart, green and integrated transport sector)
- International co-operation
- Budget: €4.99M
- Duration: 38 months (Sept. 2019 – Oct. 2022)

Introduction-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



ICCT, 2021

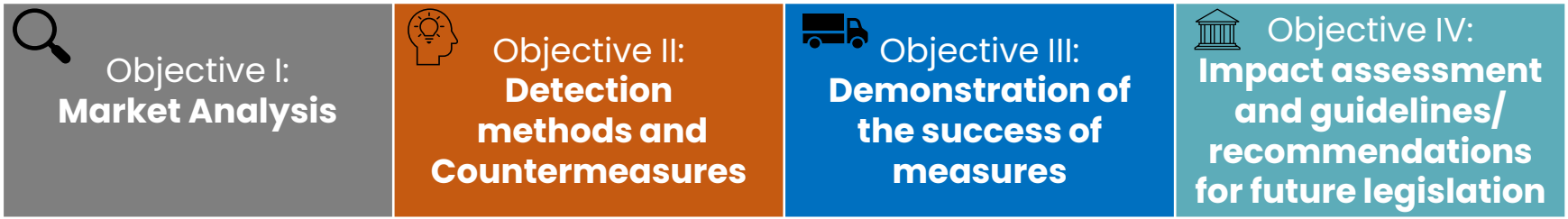
- Even a small percentage of tampered vehicles (1%) can lead to a huge increase in fleet emissions in the future (+60% for 2040)
- **Up to 10% of EU5/V and EU6/VI vehicles** in the EU are estimated to have **tampered** with environmental protection systems

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:



Objective I: Market Analysis

Overview of tampered systems and motives

Tampered Systems and Motives

SCR tampering (NOx emissions)

- Eliminate/reduce urea cost (>**€2K/truck/year**) and cost of replacing malfunctioned SCR components

DPF (GPF) tampering (PM emissions)

- Avoid the high cost of DPF replacement (>**€1.5K**), eliminate regeneration fuel penalty

EGR tampering (NOx emissions)

- Avoid the high cost of EGR-components replacement (*Note: Reduced motivation in EU6)*

TWC tampering

- *Negligible/zero for EU5/6 (Note: it was an issue for EU4)*

Objective I: Market Analysis
Overview of tampering methods

Tampering Methods

ECU reprogramming

- Manipulation of calibration values in the ECU memory
- Complex method with high cost **(from 200€)**
- Used by experienced tamperers

Emulators and “DTC clear” devices

- Provide manipulated signals and “Diagnostic Trouble Code Clear” commands to the ECU
- Low cost **(from 20 €)**
- Easy to install but with operational/reliability issues
- Applicability continuously decreasing
- Prone to visual inspection checks
- More common in HD instead of LD vehicles

Modifiers

- Simpler emulators e.g. mechanical spacers, sensor extensions, mini catalysts, resistors

Objective I: Market Analysis - Overview of DIAS testing program

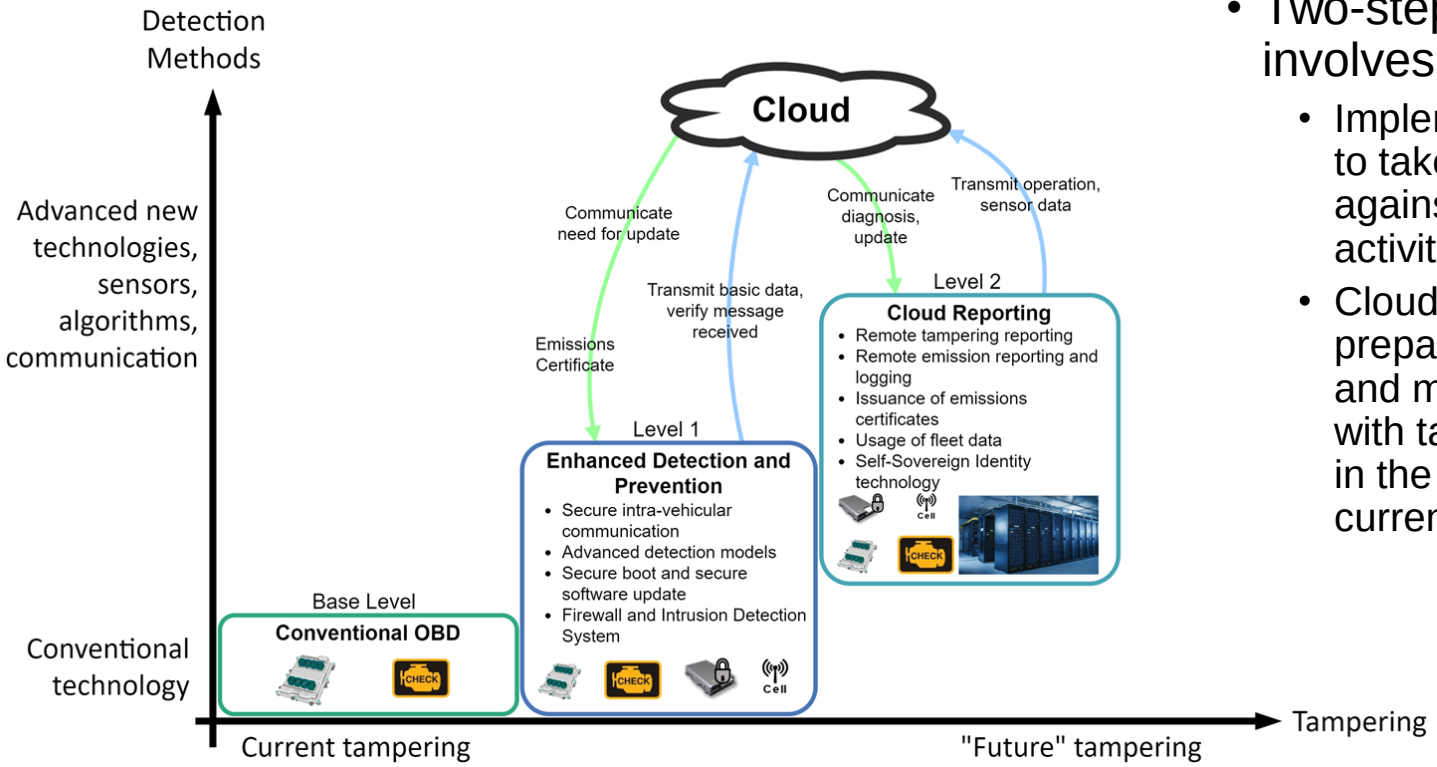
- **Test programme**: 42 commercial tampering devices/services, 5 “homemade” tampering devices:
  - Desk tests
  - In vehicle tests: 3 LDV, 3 HDV, 2 NRMM






- **Key findings:**
  - ECU flashing is considered the prevailing tampering method used in modern vehicles
  - The quality of the tampering is mixed (DTCs, malfunction indication or driver inducement for 50% of the devices/services)
  - 4 different levels of tamperers (from DIY to experts)
  - For new vehicle models, tamperers need ‘some years’ to find a reliable way to tamper the targeted system

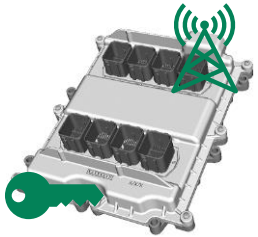
Objective II: Detection methods and countermeasures - Overview



- Two-step approach that involves:
  - Implementing measures to take early actions against tampering activities.
  - Cloud-based step that prepares methodologies and means for dealing with tampering attempts in the future that are currently unknown.

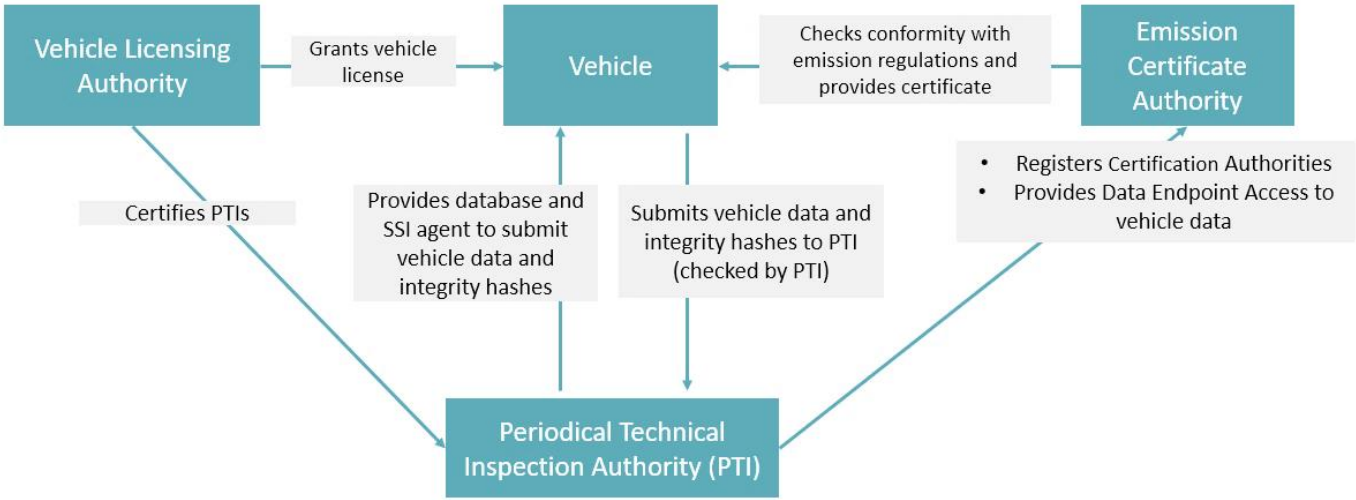
Objective II: Detection methods and countermeasures – Level 1

- Enhanced OBD system:
  - **Dedicated tampering detection** functions
  - **Advanced diagnostics** (e.g., anomaly detection) to cover more sophisticated, future emulators (also in Level 2)
- Secure in-vehicle digital communications:
  - Cryptographic key distribution protocols and techniques to authenticate **data exchanges**
  - Specially tailored protocols aimed at **digital sensors**
  - Secure CAN based on AUTOSAR SecOC specifications
- Secure boot and secure firmware update for xCUs
- Firewall and Intrusion Detection (filter malicious traffic + block tampering attempts)



Objective II: Detection methods and countermeasures – Level 2

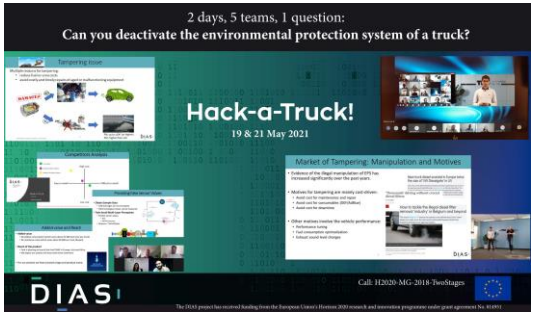
- A cloud reporting system:
  - **Input:** fleet data
  - **Output:** easily-verifiable emission certificates using Self-Sovereign Identities technology
  - **Involved parties**: Vehicle and several authorities



Objective III: Demonstration of the success of measures

- 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 *(on-going)*
  - **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

Objective IV: Impact assessment and guidelines/recommendations on future legislation – Impact assessment

- Environmental, Health and Societal

  - Address societal **needs to understand the tampering phenomenon** and generate considerable **climate** and **public health co-benefits**

Note: *A detailed Impact Assessment is currently finalizing, results will be available very soon*

- Regulatory

  - **Influence** on European and the global economy by **assessing** manipulated vehicles and **providing solutions** for **reducing** their negative **impact**
    - DIAS technical solutions are leveraged to **recommend regulatory provisions:**
      - **For vehicle manufacturers:**
        - For Type Approval of new vehicles
        - After the Type Approval for future vehicles in-service
      - **For many other end-users**

Objective IV: Impact assessment and guidelines/recommendations on future legislation – Guidelines

End users for anti-tampering:

- **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

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

- **Workshops**: Legitimate use of diagnostic tools and report tampering

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

Objective IV: Impact assessment and guidelines/recommendations on future legislation – Vehicle manufacturers' guidelines for Type Approval *(ongoing)*

Proposed functional requirements for the **Type-approval of new vehicles → Vehicle manufacturers should:**

1. Perform a Threat Assessment and Risk Analysis (TARA), and market analysis for:
- Components (sensors, control units): flashed, emulated, modified
- In-vehicle communication/data exchange: no integrity, no authenticity
- Vehicle-to-Infrastructure (V2I) communication/data exchange

2. Develop countermeasures for prevention and detection which must:
- Cover the fundamental requirements which have been identified by DIAS
- Be proportional based on the TARA
- Be adaptable based on the market analysis

3. Provide tampering-related reporting methods for:
- In-vehicle reporting (e.g. MIL-type)
- V2I reporting (e.g. reporting to a cloud infrastructure)

4. Develop methods for inducement and enforcement of repair

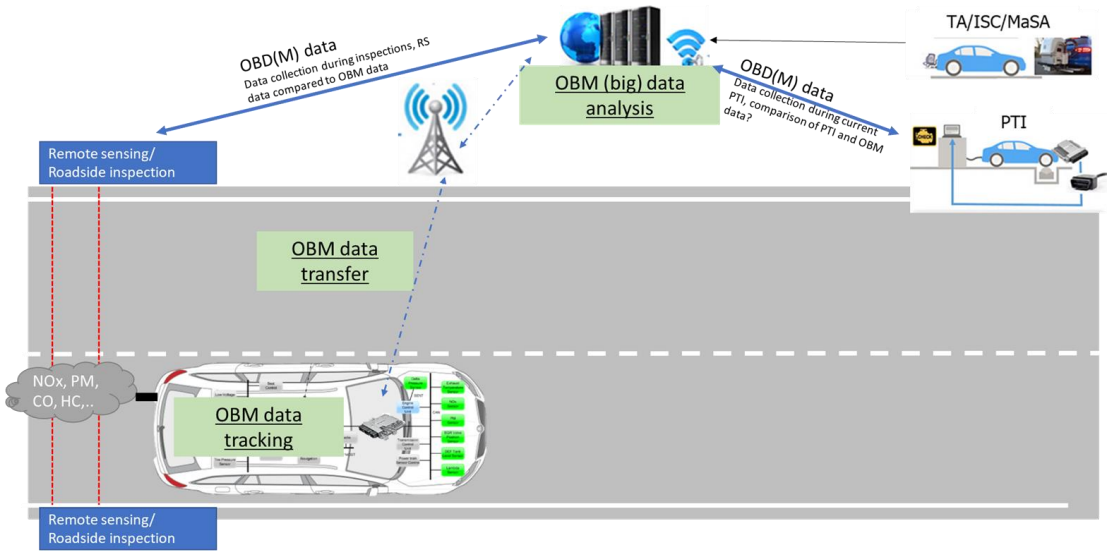
5. Demonstrate/declare conformity wth the legislative requirements

Objective IV: Impact assessment and guidelines/recommendations on future legislation – Vehicle manufacturers' guidelines after Type Approval *(ongoing)*

- Proposed functional requirements **after the Type Approval (for future vehicles in service) → Vehicles manufacturers should:**
  - Follow up on:
    - Evidences and information from the tampering market
    - Feedback from vehicle dealers/workshops
    - Feedback from periodical technical inspections (PTI)
    - Test results from in-service conformity testing or market surveillance tests (ISC and MaS)
    - Road-side inspections
  - Repeat the TARA and develop/update the countermeasures to mitigate the new threats

Objective IV: Impact assessment and guidelines/recommendations on future legislation – Overview of future regulatory framework

- **Future emission compliance framework** for vehicles is expected to combine information and data from the vehicle, the roadside inspection, the Periodic Technical Inspection and the vehicle's Type Approval
- **Anti-tampering is an important prerequisite** for effective and reliable vehicle data and policies (e.g. OBM)
- Several end-users should be engaged
- **Expectations for Type Approval: EU7 legislation will include specific anti-tampering guidelines**



Summary

- Even a small number of tampered vehicles can lead to a remarkable increase in fleet emissions *(note: actual number of tampered vehicles may be underestimated today)*
- ECU tampering is the main concern today
- Developed solutions are in 3 directions: diagnostics, security and reporting
- Successful anti-tampering should engage several end-users; DIAS focuses on guidelines for vehicle manufacturers and covers many other end-users
- Legislative framework should:
  - Cover both the Type Approval of vehicles and vehicles in-service
  - Combine information and actions for all involved end-users

Thank you

Dr. Dimitrios Kontses
Aristotle University of Thessaloniki, Greece
Tel: +302310.990543
E-mail: dkontses@auth.gr

Prof. Zissis Samaras
Aristotle University of Thessaloniki, Greece
Tel: +302310.996014
E-mail: zisis@auth.gr

dias-project.com