DIAS

Smart Adaptive Remote Diagnostic Anti-tampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D6.5
Deliverable Title	Impact assessment and guidelines for future anti-tampering regulations
Issue Date	16/11/2022
Dissemination level	Public
Main Author(s)	Dimitrios Kontses
	Alexandros Papageorgiou-Koutoulas
	Sina Kazemi Bakhshmand
	Pierre-Louis Ragon
	Eamonn Mulholland
	Robin Vermeulen
	Iddo Riemersma
	Odysseas Bakatselos
	Dimitrios Gkliagias
Version	V1.0

DIAS Consortium

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

Document log

Version	Description	Distributed for	Assigned to	Date
v0.1	Draft structure of deliverable	Structure review	Core Group (CG) members	15/06/2022
v0.3	Draft content of deliverable and partner inputs	Content review	BOSCH, FEV	03/08/2022
v0.4-v08	Draft content of deliverable and partner inputs v2	Content review	BOSCH, FEV	September 2022
v0.8-v0.9	Reviewer's comments addressed	GA check	GA members	12/10/2022
v1.0	First final version	-		

Verification and approval of the final version

Description	Name	Date
Verification of the "Final content of deliverable (v0.9)" by WP leader	Dinitrios Kontses	10/11/2022
Check of the "First final version (v1.0)" before uploading by coordinator	Zissis Samaras	16/11/2022

Executive summary

Tampering attempts at automotive environmental protection systems (EPS) result in elevated tailpipe emissions up to uncontrolled levels of vehicles of decades ago, contributing to poor air quality and adverse effects on human health. DIAS project, funded by the European Union (EU) Research and Innovation program Horizon 2020, aims to harden vehicles' EPS against tampering by fulfilling 4 main stepwise objectives:

I. **Analyse the "Market" and assess** the operation of representative tampering systems and their effect on the performance of existing on-board emission monitoring and emission control systems over real-world and laboratory testing
II. **Develop countermeasures** to prevent, detect and report tampering
III. **Test and demonstrate** the success of the countermeasures
IV. **Propose a set of guidelines and recommendations** for future legislation for the introduction of efficient ant-tampering countermeasures

This report addresses the 4th DIAS objective by presenting an anti-tampering framework that incorporates guidelines and recommendations for future anti-tampering legislation based on the findings during the whole period of the project. Options are also provided for compliance confirmation with regulatory requirements to achieve effective development and implementation of countermeasures on new vehicles and vulnerability management for vehicles in-service. Additionally, the environmental, health, and monetary impact of tampering is investigated across the European light- and heavy-duty vehicle (LDV, HDV) fleet, while the potential benefit of anti-tampering legislation (by reducing the negative impact) is considered.

Impact Assessment

Focusing on particulate matter (PM) and nitrogen oxides (NOx) emissions as the two pollutant emissions which are most negatively affected by EPS tampering and due to scarce data for other pollutants, total emissions from the on-road vehicle fleet and the share attributable to tampered vehicles were estimated based on tampering inputs available and vehicle stock model. The public health burden associated with tampering was estimated based on the Fast Assessment of Transportation Emissions (FATE) model. Several scenarios were determined to address data limitations and to cover a wide range of tampering incidence and emission factors. The central estimation scenario reflects the best estimate for the tampering shares and tampering rates based on evidence from different roadside inspections and remote sensing emission measurement campaigns in Europe. Based on this scenario, over the 2022-2050 period, compared to no tampering case, tampering leads to roughly:

- 3.7 megatonnes (or 20%) additional NOx emissions. Assuming a faster transition to zero-emissions vehicles (ZEVs) for HDVs the impact is only slightly reduced.
- 41 kilotonnes (or 12%) additional PM emissions. Assuming a faster transition to ZEVs for HDVs the impact is reduced to 29 kilotonnes (or 8%).
- 26,000 additional premature deaths. Assuming a faster transition to ZEVs for HDVs this value is reduced to 21,000.
- 460,000 additional years of life lost. Assuming a faster transition to ZEVs for HDVs this value is reduced to 380,000.

Half impact is estimated based on the best-case (adopting the lowest tampering shares and rates) and double to triple for the worst-case (adopting the highest tampering shares and rates) scenario.

These results represent the maximum theoretical benefits that can be achieved in an ideal case where 100% of the tampering is eliminated by the introduction of anti-tampering legislation. Considering this fact, anti-tampering regulation can deliver a significant contribution to mitigating the health and environmental impacts of road transport.

Anti-tampering guidelines

The current European Union (EU) and United Nations Economic Commission for Europe (UNECE) vehicle emissions-related legislation (including both regulations and directives) incorporates a few anti-tampering measures, but still, significant gaps and limitations remain that tamperers exploit. These are relevant to:

- **Tampering-related monitors and obligations towards Original Equipment Manufacturers (OEMs), workshops, and vehicle owners**: Existing monitors and obligations address only a part of tampering attacks
- **Tampering definition**: Explicit definition is missing from some basic regulations e.g. (European Parliament, Council of the European Union, 2007)
- **Reporting**: e.g. EU laws regulate vehicle data exchange among Member States (MS) and between MS and EC. However, no reference or obligation is found regarding tampering-proof reporting or tampering-specific data to be transferred/reported.
- **Prohibitions and penalties:** e.g. The use, execution, or trade of tampering-related devices/services (including not-approved by relevant authorities, and in turn tampering-suspicious, aftermarket parts) only partly and not explicitly forbidden and penalized.
- **Roadworthiness inspections:** Only a few specific requirements are currently set regarding tampering-relevant checks and reporting implemented by Periodic Technical Inspection (PTI) centres and Roadside Inspection (RSI) authorities authorities

The DIAS project focused on providing technical solutions for tampering prevention, detection, and reporting. Based on these solutions, the functional requirements to be applied from OEMs were extracted. A functional requirement means that the objective of the legislative requirement is described in qualitative terms of what it should be achieved, while it is left open to the vehicle OEMs to choose the means to realize this objective upon approval by the authority. In this way, the technology neutrality of the guidelines is retained while stimulation is raised to apply the most cost-effective anti-tampering solution. Relative technical details, where needed, are documented only as technical examples. The proposals for OEMs [also integrating the role of Type approval authorities (TAA)] are summarized as:

- **For the type-approval of new vehicles**: Implement functional requirements for the development of specific countermeasures for vulnerabilities that can be foreseen. This includes the following elements:
    a. Threat Analysis and Risk Assessment (TARA) and market analysis
    b. Dedicated countermeasures
        - Countermeasures derived from TARA and market analysis
        - Fundamental countermeasures
            - Secure data exchange between specific SCUs and ECU
            - Secure ECU flashing
            - Identification of executed software
            - Frequent FCM clear detection
            - Estimation of tampering indicator value

    - Other countermeasures
  c. Tampering-related and secure reporting
  d. Inducement and enforcement of repair
  e. Demonstration and declaration of conformity with legislative requirements
- **For vehicles in-service**: Implement a functional requirement that prompts the OEM to follow up on signs from the market that tampering might be taking place by managing threats by a cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating threats i.e. developing upgrades for the countermeasures and the inducement of vehicles (vulnerability management). This includes the following elements:
  a. General statement on tampering prevention
  b. Proactive monitoring of vehicle fleet
  c. Allow third parties to supply tampering evidence

Generic guidelines regarding the other involved parties were also provided:

- **MS**:
  - Prohibition and relevant fines for use, execution, or trade of tampering-related devices, services, and practices and liability definition in each case
  - Legislating and enforcement of tampering-relevant checks and reporting by roadworthiness inspections
  - Enforcement to report any tampering case and provision of reporting options (exception: OEMs where a different procedure is proposed)
- **PTI centres and RSI authorities**:
  - Advanced emission measurement techniques for all regulated pollutants
  - Advanced visual inspections
  - Access and evaluation of tampering-related data
  - Reporting of tampered vehicles
  - Enforcement actions
- **Workshops**:
  - Expansion of the SERMI scheme to protect access to EPS-related information
  - Voluntary submission of tampering-related information
- **In-Service Conformity (ISC), Market Surveillance (MaS), (Remote Sensing) authorities**:
  - Advanced visual inspections
  - Reporting of tampered vehicles
  - Reporting of vehicles with high emissions but with inactive MIL and under investigation from Granting Type Approval Authorities
- **Vehicle owners**: Burdened with fines, costs for EPS reversion to its original form, testing costs or other penalties, if liable for any tampering case

Contents

List of Abbreviations

Abbreviation	Full term
AECC	Association for Emissions Control by Catalyst
CAL ID	Calibration identifier
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CARB	California Air Resources Board
CCR	California Code of Regulations
CCU	Connectivity Control Unit
CDM	Consumption Deviation Monitor
CFR	US Code of Federal Regulations
CG	Core Group
CH_4	Methane
CITA	International Motor Vehicle Inspection Committee (Comité international de l'inspection technique automobile)
CLOVE	Consortium for ultra-Low Vehicle Emissions
CO	Carbon Monoxide
CO_2	Carbon Dioxide
CRL	Certificate Revocation List
CRT	Continuously Regenerating Trap
CSR	Certificate Signing Request
CVN	Calibration Verification Number
CVSS	Common Vulnerability Scoring System
DALY	Disability-adjusted life years
DCU	Dosing Control Unit
DEF	Diesel Exhaust Fluid (AdBlue™)
DENM	Decentralized Environmental Notification Message
DH	Diffie-Hellman
DIAS	Smart adaptive remote DIagnostic Antitampering Systems
DID	Decentralized Identifier

DOC	Diesel Oxidation Catalyst
DoW	Description of Work
DPF	Diesel Particulate Filter
DTC	Diagnostic Trouble Code
EC	European Commission
ECDH	Elliptic Curve Diffie-Hellman
ECE	Economic Commission for Europe
ECU	Engine Control Unit
EGR	Exhaust Gas Recirculation
ENISA	European Union Agency for Cybersecurity
EPA	United States Environmental Protection Agency
EPS	Environmental Protection System
EU	European Union
FATE	Fast Assessment of Transportation Emissions
FCM	Fault Code Memory
FNR	False Negative Rate
FPR	False Positive Rate
GA	General Assembly
GBD	Global Burden of Disease
GNSS	Global Navigation Satellite System
GPF	Gasoline Particulate Filter
GST	Generic Scan Tool
GTR	Global Technical Regulations
GVWR	Gross vehicle weight rating
H_2O	Water
HC	Hydrocarbons
HDV	Heavy-Duty Vehicle
HDVIP	heavy-Duty Vehicle Inspection Program
HEGO	Heated Exhaust Gas Oxygen (sensor)

ICCT	International Council on Clean Transportation
ICSMS	Information and Communication System on Market Surveillance
IDS	Intrusion Detection System
IO	Independent Operator
IP	Internet Protocol
ISC	In-Service Conformity
ISO	International Organization for Standardization
KDK	Key Distribution Key
KFG	Austria's Federal Act governing automotive engineering (Kraftfahrgesetz)
LDV	Light Duty Vehicle
LNT	Lean NOx Trap
LOKI	Lightweight Cryptographic Key Distribution Protocol
MAC	Message Authentication Code
MECS	Microbial Electrolysis Cells
MIL	Malfunction Indication Lamp
MS	Member State
N_2	Nitrogen
N_2O	Nitrous oxide
NH_3	Ammonia
NO	Nitric oxide
NO_2	Nitrogen dioxide
NO_x	Nitrogen Oxides i.e. NO and NO_2
NPTI	New Periodic Technical Inspection
NRMM	Non-Road Mobile Machinery
NTE	Not-To-Exceed testing
NVRAM	Non-Volatile Random Access Memory
O_3	Ozone
OBD	Onboard Diagnostics
OBFCM	Onboard Fuel Consumption Monitoring

OBM	Onboard Monitoring
OC	Organic Carbon
ODR	Operating Data Recorder
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection
OTA	Over The Air
OWASP	Open Web Application Security Project
PAS	Publicly Available Specification
PCM	Pulse-code Modulation
PEMS	Portable Emission Measurement System
PM	Particulate Matter
$PM_{2.5}$	Fine inhalable particles, with diameters that are generally 2.5 micrometres and smaller
PN	Particulate Number
PSIP	Periodic Smoke Inspection Program
PTI	Periodical Technical Inspection
RA	Registration Authority
RAPEX	Rapid Information System
RDE	Real Driving Emissions
RMI	Repair and Maintenance Information
RoT	Root of Trust
RPM	Rotations Per Minute (engine speed)
RSI	Roadside Inspection
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
SAE	Society of Automotive Engineers
SCR	Selective Catalytic Reduction
SCU	Sensor Control Unit
SEMS	Smart Emission Measurement System

SERMI	Forum for access to security-related vehicle repair and maintenance information
SK	Session Key
SP	Service Provider
SRK	Storage Root Keys
SSI	*Self Sovereign Identity*
SUMS	Software Update Management System
SW	Software
TAA	Type Approval Authority
TARA	Threat Analysis and Risk Assessment
THC	Total Hydrocarbons
TPM	Trusted Platform Module
TWC	Three Way Catalyst
UK	United Kingdom
UN	United Nations
UNECE	United Nations Economic Commission for Europe
US	United States
V2I	Vehicle to infrastructure
V2X or X2V	Vehicle to everything
VECTO	Vehicle Energy Consumption calculation TOol
VGT	Variable-geometry turbocharger
VKT	Vehicle-kilometres travelled
VLA	Vehicle License Authority
VVT	Variable valve timing
WHSC	World Harmonized Stationary Cycle test
WHTC	World Harmonized Transient Cycle test
WLTP	Worldwide harmonized Light vehicles Test Procedure
WP	Work Package
xCU	Any electronic control unit used in automotives e.g. engine, connectivity, sensor, telematic control units
ZEV	Zero-Emission Vehicles

List of Definitions

Term	Definition
(Technological) Complexity	Criterion to evaluate the needed technological level for the design and manufacture of a solution, considering its characteristics and performances.
AdBlue™/DEF	An aqueous urea solution made with 32.5% urea and 67.5% deionized water. DEF is consumed in SCR that lowers nitrogen oxides (NOx) concentration in the diesel exhaust emissions from a diesel engine.
Aftermarket parts	Replacement parts that are not made by the original manufacturer. Aftermarket parts are used to replace damaged parts in vehicles and other equipment. They are typically cheaper than OEM parts but are likely to have a similar effect.
Attack vector	A method or pathway used by an attacker to access or penetrate the target system (in cybersecurity).
Attacker	An individual who attempts to access the vehicle's network, mostly without the owner's consent.
Authentication	Verifying the identity of a person or a communication partner.
Authority	Person or body having the legal power to make and enforce the law. With regard to the legislation on vehicle emissions and environmental protection systems the following types of authorities are involved: - Development of regulations and norms, like the UNECE. Typically, a global or international organisation. - Enforcement of regulations and norms, like approval authorities such as the RDW or DVSA. Usually organised per country or Member State.
Cost	Criterion to evaluate the estimated financial resources needed for development (including new production lines needed) and operation of the technology used.
Customer	A person who buys goods or services from a shop or business. With regard to environmental protection systems the distinction can be made between: - Customer: a person who buys goods or services without the intention of tampering with the environmental protection systems. This includes the uninformed customer: who believes no tampering is involved while in fact it is. - Intentional customer: a person who buys goods or services with the intention to tamper with the environmental protection systems of the vehicle.
Data integrity	The receiver of data must have the assurance that the data has come intact from the intended sender and has not changed intentionally or unintentionally. This is ensured through the use of secure hash algorithms.
DIDComm	A standard that defines the secure and authenticated communication channel between Decentralized Identifier (DID)-controlling entities.
DPF or FAP	A device designed to remove diesel particulate matter or soot from the exhaust gas of a diesel engine. DPF is used in modern diesel vehicles and NRMM.
ECU	A type of electronic control unit that controls a series of actuators on an internal combustion engine to ensure optimal engine performance.
ECU flashing	Electrical operation of reprogramming an ECU memory.

EGR	A NOx emissions reduction technique used in gasoline and diesel engines. EGR works by recirculating a portion of an engine's exhaust gas back to the engine cylinders. This dilutes the O2 in the incoming air stream and provides gases inert to combustion to act as absorbents of combustion heat to reduce peak in-cylinder temperatures.
Emulator	A device intended to take over control of a tampered EPS.
End-user	End-users include everyone who should be involved in the application of anti-tampering practices. The definition includes at least manufacturers and regulators. The definition may be extended to include the law-abiding workshops and vehicle owners who assist the anti-tampering practices.
EPS	System fitted to a vehicle that is designed to reduce any (pollutant) emissions of that vehicle, e.g. EGR, DPF and SCR.
Firewall	A software module that monitors the network traffic (in the case of the DIAS project both CAN, and IP communications), and uses a set of rules to control incoming and outgoing traffic.
Functional requirements	A set of requirements defining in qualitative terms what the vehicle should fulfil, but the way in which this is realised is left open to the vehicle manufacturer upon approval by the authority. A functional requirement is not restrictive towards any solution that fulfils the objective, and the chosen approach is based on the performance in practice (ex-post approach).
GEOS-Chem	A global 3-D model of atmospheric chemistry driven by meteorological input and used by researchers around the world to assess a variety of atmospheric composition problems
GPF/OPF/PPF	A device designed to remove particulate matter or soot from the exhaust gas of a gasoline engine.
Heavy-Duty	Vehicles that meet the requirements of vehicle categories M2, M3, N2 and N3 as defined in directive 2007/46/EC which involve: · M2 and M3: Vehicles designed and constructed for the carriage of passengers, comprising more than eight seats in addition to the driver's seat, and having a maximum mass not exceeding 5 tonnes for M2 and exceeding 5 tonnes for M3. · N2 and N3: Vehicles designed and constructed for the carriage of goods and having a maximum mass exceeding 3,5 tonnes but not exceeding 12 tonnes for N2 and having a maximum mass exceeding 12 tonnes for N3.
Intrusion detection system	In the case of the DIAS project, it is a software module that monitors the network traffic (e.g., CAN frames), and uses a signature database (i.e., rule file) to detect malicious activity.
Lead time	Criterion to evaluate the amount of time that passes from the start of developing a solution until its conclusion.
Light-Duty	Vehicles that meet the requirements of vehicle categories M1 and N1 as defined in directive 2007/46/EC which involves: - M1: Vehicles designed and constructed for the carriage of passengers and comprising no more than eight seats in addition to the driver's seat. - N1: Vehicles designed and constructed for the carriage of goods and having a maximum mass not exceeding 3,5 tonnes.

Low hanging fruit	Any anti-tampering solution which is simple in concept, low-cost and short-term available.
Manufacturer or OEM	Person or body that makes goods for sale. With regard to vehicle manufacturing and especially environmental protection systems the distinction can be made between: - Manufacturer: a person or body who is responsible to the approval authority for all aspects of the type-approval or authorisation process and for ensuring conformity of production. It is not essential that the person or body be directly involved in all stages of the construction of the vehicle, system, component or separate technical unit which is the subject of the approval process, as defined in directive 2007/46/EC. - Tampering manufacturer: person or body that constructs a tampering device.
NRMM	Non-Road Mobile Machinery. Any self-propelled vehicle which is designed and constructed specifically to perform work, which, because of its construction characteristics, is not suitable for carrying passengers or for transporting goods, as defined in directive 2007/46/EC. Machinery mounted on a motor vehicle chassis shall not be considered mobile machinery.
OBD (system)	A system that continually monitors the electronic sensors of engine and EPS subsystems. When a potential problem is detected, a dashboard warning light (MIL) is illuminated to alert the driver. Note that the OBD is not originally intended to detect malicious alterations of the system.
Periodical Technical Inspection authority (PTI)	The PTI is a fictional name for an authority, which is allowed to collect vehicle data (e.g. related to NOx emissions) in the context of the solution proposed in this DIAS report.
SCR	A means of converting NOx with the aid of a catalyst into N2 and H2O. SCR is used in modern diesel vehicles. A gaseous reductant, typically anhydrous ammonia, aqueous ammonia, or urea is added to a stream of flue or exhaust gas and is adsorbed onto a catalyst. Carbon dioxide, CO2 is a reaction product when urea is used as the reductant.
Secure logging	The generated logs are signed via a secret key.
Supplier	Person or body that provides something needed such as a product or service. With regard to environmental protection systems the following distinction can be made for suppliers: - Supplier: Vendors or workshops/repair shops that provide a product or service regarding all stages of the construction of a vehicle, system, component or separate technical unit in a vehicle without involvement in any tampering related device or service. - Tampering supplier: Vendors or workshops/repair shops that provide tampering devices, tools and/or the service to tamper with environmental protection systems.
Tamperer	A person who intentionally, illegally and for whatever reason alters an EPS, resulting in increased emissions.
Tampering Device	Also known as a cheating device. A system, component or separate technical unit that, when fitted to a vehicle, actively or passively tampers with an environmental protection system of a vehicle with the purpose of (partly) deactivating or bypassing it. This typically includes the removal or deactivation

	of systems in a vehicle that monitor the status of those environmental protection systems and give feedback about malfunctions, i.e. the OBD system of the vehicle.
Tampering rate	The ratio of tampered to non-tampered vehicle emissions
Tampering Service	A service provided by a supplier or tamperer to make changes to an environmental protection system or ECU with the purpose of (partly) deactivating or bypassing it. This typically includes the removal or deactivation of systems in a vehicle that monitor the status of those environmental protection systems and give feedback about malfunctions.
Tampering share	Share (in %) of the tampered vehicles in the vehicle fleet of a region e.g. European fleet
Technical requirements	A prescribed set of clear requirements and/or type approval tests with specific limits that the vehicle should fulfil. The underlying assumption is that if the vehicle which is type approved complies with these technical requirements, the production vehicle will also comply (ex-ante approach).
Technology neutrality and applicability industry-wide	Criterion to evaluate whether the basic principle of the solution can be used in all vehicles and does not require technology-specific know-how, but build upon existing common automotive technology, logical controls, statistical functions, mathematical functions and physical laws.
To tamper	Interfere with something to cause damage or make unauthorised alterations.
Trusted platform module	A security controller that is compliant with the TPM 2.0 specification.
TWC	A catalyst that oxidizes hydrocarbons (CxHy), CO and NOx into N2, CO2 and H2O. The catalyst is used in gasoline vehicles.
Type approval	The procedure whereby a Member State certifies that a type of vehicle, system, component, or separate technical unit satisfies the relevant administrative provisions and technical requirements as defined in directive 2007/46/EC.
Type Approval Authority	The authority of a country or Member State with competence for all aspects of the approval of a type of vehicle, system, component, or separate technical unit or of the individual approval of a vehicle; for the authorisation process, for issuing and, if appropriate, withdrawing approval certificates; for acting as the contact point for the approval authorities of other Member States; for designating the technical services and for ensuring that the manufacturer meets his obligations regarding the conformity of production. As defined in directive 2007/46/EC.
V2I	Vehicle to infrastructure (V2I) refers to the wireless exchange of data between the vehicle and surrounding infrastructure, such as traffic lanes, signs, lights, or a cloud infrastructure.
V2X	Vehicle-to-everything (V2X) refers to the communication of a vehicle to any entity that may be affected by the vehicle (such as an application in the cloud).
VLA	Vehicle Licensing Authority (VLA) is a fictional name for an authority, which is allowed to register vehicles in the context of the solution proposed in this DIAS deliverable D4.3.
Vulnerability	A weakness that can be exploited by a threat, such as an attacker

xCU	Used to refer to the different Electronic Control Units (ECUs) of a vehicle, where “x” stands for whichever of the electronic control unit modules (e.g. Powertrain Control Unit – Pulse-code Modulation (PCM), Transmission Control Unit – TCM etc.)

List of Figures

List of Tables

1 Introduction

1.1 Background

The European Green Deal is a new growth strategy for the European Union (EU) which has introduced a zero-pollution ambition for Europe. Recognizing the contribution of transport to air pollution, the European Green Deal has a strong desire that transport becomes drastically less polluting, especially in cities. As part of this strategy, the European Commission (EC) aims at ensuring secure vehicle environmental protection systems from tampering and in turn emission compliance to the latest "Euro" vehicle emission standards and On-Board Diagnosis (OBD) legislation. The Diagnostic Anti-tampering System (DIAS) project was funded by the EU Research and Innovation program Horizon 2020 to contribute to this target.

The main DIAS stepwise objectives are to:

- **Analyze the "Market" and assess** the operation of representative tampering systems and their effect on the performance of existing on-board emission monitoring and emission control systems over real-world and laboratory testing
- **Develop countermeasures** to prevent, detect and report tampering
- **Test and demonstrate** the success of the countermeasures
- **Propose a set of guidelines and recommendations** for future legislation for the introduction of efficient ant-tampering countermeasures

1.2 Main objectives

This study covers the objectives of two tasks:

- Task 6.3 - Guidelines for anti-tampering legislation, targeting to:
    - Develop and propose a set of guidelines and recommendations for future anti-tampering legislation. The proposed guidelines were developed targeting both heavy-duty vehicles (HDVs) and light-duty vehicles (LDVs) and they are formed in a uniform and technology-neutral way.
    - Assess the environmental and health impact of tampering
- Task 3.3: Type approval test protocol for legislative context, targeting to:
    - Confirm compliance with regulatory requirements to achieve effective implementation of countermeasures on new vehicles and vulnerability management for vehicles in-service While testing has proven not always to be effective in the past, other options should be considered as well.

1.3 Deliverable structure

This deliverable is organized into six basic chapters:

- Chapter 1 provides the background, goals, and structure of this deliverable.
- Chapter 2 contains the tampering environmental, health, and monetary impact assessment under different modelling scenarios. The potential benefit of anti-tampering legislation is also evaluated, using the model forecast results.

- Chapter 3 introduces the anti-tampering framework and defines its basic structure and components
- Chapter 4 presents the anti-tampering guidelines, in terms of functional requirements, addressed to vehicle manufacturers (OEMs)
- Chapter 5 presents the anti-tampering guidelines addressed to the rest involved parties in anti-tampering
- Finally, chapter 6 concludes the purposes and summarizes the findings of this report

1.4 Deviations from original Description of Work (DoW)

1.4.1 Description of work related to deliverable as given in DoW

In the DoW, the description of the deliverable D6.5 in *Grant Agreement-814951-DIAS (p. 115)* is the following:

"This report will contain a legislative text and arguments to support the introduction of future legislation and will be open to the public."

The current document comprises also D3.3 deliverable content. The relevant description of the D3.3 deliverable found in *Grant Agreement-814951-DIAS (p. 99)* is the following:

"A report on the test protocol to be used in a legislative context."

1.4.2 Time deviations from original DoW

No delay

1.4.3 Content deviations from original DoW

This document incorporates two complementary tasks:

- T3.3: Anti-tampering test protocol for use in future type approval test
- T6.3: Guidelines, impact assessments, and text for future legislation.

The title of the deliverable was adjusted to better reflect its content. In particular, instead of "Guidelines, impact assessments and text for future legislation", the deliverable was entitled as "Impact assessment and guidelines for future anti-tampering regulations". During the development phase of the regulatory requirements, it was realized that an effective anti-tampering framework should engage many additional end-users apart from the OEMs which was initially the plan for this task. Thus, we broaden the scope of our study to include requirements for all involved end-users instead of focusing only on the requirements for the Type Approval legislation.

There are no further content deviations from the original DoW.

2 Impact assessment

The aim of the present impact assessment is to investigate the emissions and health impacts of tampering across the European light- and heavy-duty vehicle fleet. A modelling exercise is performed using the International Council on Clean Transportation (ICCT)'s in-house tools to estimate the environmental impact of tampering given the best available data, the associated air quality-related health issues, the potential of anti-tampering solutions in reducing this negative health impact, and the economic implications of regulating anti-tampering solutions. The EU is considered a single market and the European fleet is therefore modelled as one entity. Passenger cars, trucks, and buses are modelled separately.

2.1 Sources and Methodology

2.1.1 Modelling method

A two-stage modelling approach is adopted to estimate the health impacts of tampering. First, total emissions from the on-road vehicle fleet are estimated and the share attributable to tampering under several scenarios is determined. Second, the air quality and health impacts attributable to the additional emissions from tampered vehicles are estimated. The method and models used are summarized in Figure 2-1 and described below. The vehicle stock modelling is described in 2.1.2, while the inputs and scenarios used for tampering modelling are covered in sections 2.1.3 and 2.1.4, respectively. Emissions modelling results from the Roadmap model are covered in section 2.2. Finally, section 2.3 covers the health impact calculations using the FATE model.

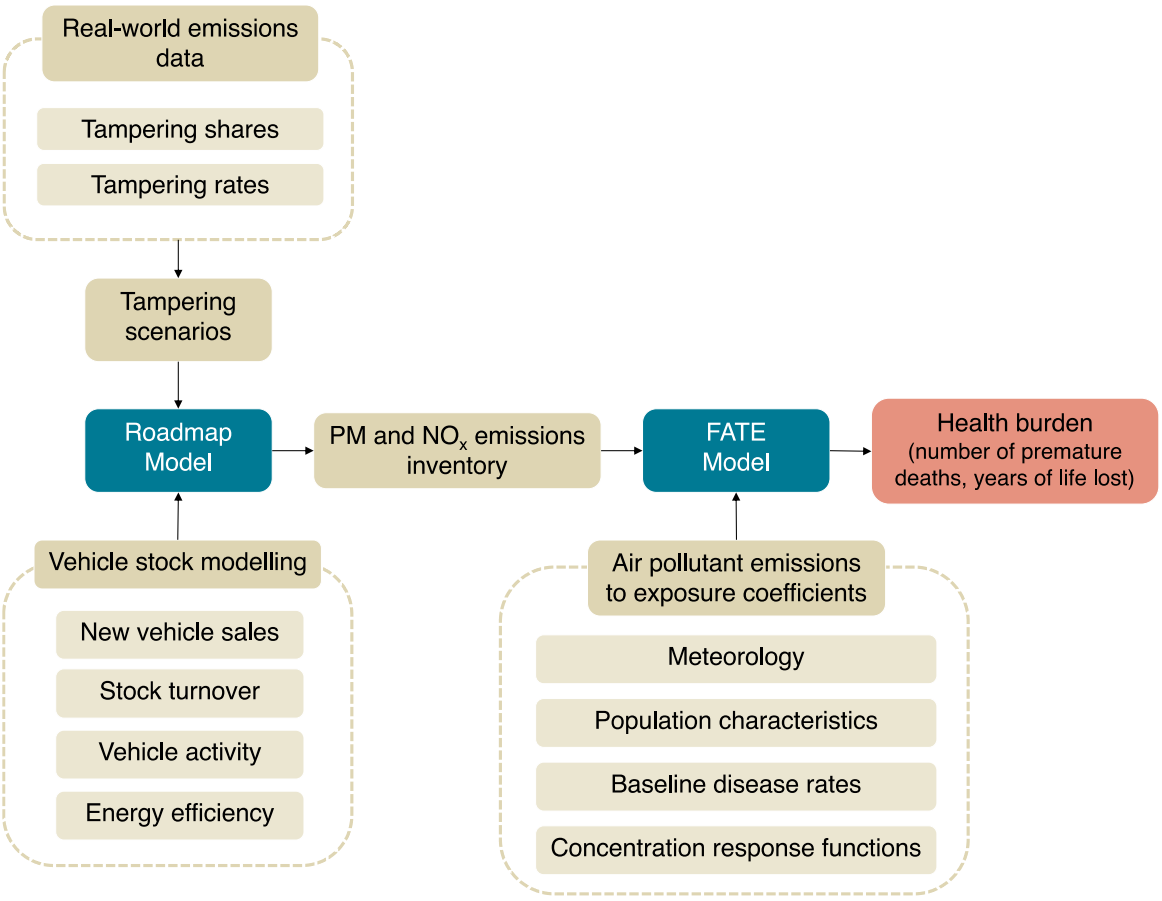


Figure 2-1: Modelling method used to estimate the emissions, air quality and health impacts of tampering in on-road vehicles

In the first modelling stage, ICCT's Roadmap model is used to estimate the total air pollutant emissions in the EU out to 2050, based on modelling of the vehicle stock as well as data on vehicle activity, fuel type, and energy efficiency. Roadmap is a global transportation emissions inventory model covering all on-road vehicle activity and calculating both historical and projected emissions of several air pollutants and CO_2 emissions (Transportation, ICCT's Roadmap Model Documentation, 2021). The focus of the present work is on particulate matter (PM) and nitrogen oxides (NO_x) emissions, as the two pollutant emissions which are most affected by tampering with the emission control systems.

The second stage of the modelling estimates the public health burden associated with tampering, based on the emissions data generated with Roadmap, using the Fast Assessment of Transportation Emissions (FATE) model (Transportation, FATE v0.3 Documentation, 2021). FATE uses coefficients derived from iterative runs of the GEOS-chem model[1] to calculate the effects of gridded air pollutant emissions on population-weighted exposure to ambient concentration of particulate matter ($PM_{2.5}$) and ozone (O_3) pollutants and the associated health impacts. The main health impacts associated with NOx emissions assessed here are through its contributions to the formation of $PM_{2.5}$ and O_3. The impacts of direct

[1] GEOS-Chem is a global 3-D model of atmospheric chemistry driven by meteorological input and used by researchers around the world to assess a variety of atmospheric composition problems.

exposure to nitrogen dioxide (NO_2) are not covered in this analysis. FATE then evaluates the health impacts related to exposure to these ambient pollutants. The two key metrics used to assess health impacts are the number of premature deaths, and the number of years of life lost due to premature deaths. The method used here is in line with the latest methodology of the Global Burden of Disease (GBD) study (Global Burden of Disease (GBD), 2020).

The contributions of tampering to overall NO_x and PM emissions, and eventually to the public health burden, are determined by modelling the incidence and resulting emission levels associated with tampering, based on inputs described in the following sections.

2.1.2 Vehicle stock modelling

The modelling of the vehicle stock follows projections for the uptake of zero-emission vehicles (ZEVs) driven by currently adopted policies, and projections for the implementation of more stringent pollutant emission standards for internal combustion engine vehicles. For light-duty vehicles, an agreement has been found between the European Commission, European Parliament, and Council to revise the stringency of the CO_2 standards and mandate a 100% reduction in CO_2 emissions for new vehicles in 2035, with an intermediate reduction target of 55% for passenger cars and 50% for vans in 2030 (Commission, 2022). Therefore we model a ZEV uptake in line with these new targets. For heavy-duty vehicles, ZEV sales are modelled to follow the sales levels mandated by the current HDV CO_2 standards, mandating CO_2 emissions reductions in new vehicles of 15% in 2025 and 30% in 2030 compared to a 2019-2020 baseline (European Commission 2019). This results in a projected combined ZEV stock share of 12% in 2030, 30% in 2040 and 38% in 2050 (Eamonn Mulholland J. M.-L., 2022).

Besides, for the remaining internal combustion engine vehicle stock, the Euro 7/VII pollutant emission standard currently under development is assumed to be implemented in 2027, for both light- and heavy-duty vehicles, progressively replacing vehicles certified to older standards (Eamonn Mulholland J. M., 2021). The resulting vehicle stock projections out to 2050, by emission standard, are plotted in Figure 2-2.

The CO_2 regulation for heavy-duty vehicles is in the process of being revised to a higher level of stringency, which is expected to result in a faster and wider deployment of ZEVs. Under a scenario that follows the ambitions announced by European automobile manufacturers, this is expected to result in a projected ZEV stock share of 14% in 2030, 60% in 2040 and 90% in 2050, as shown on the bottom panel of Figure 2-2. Such an accelerated ZEV uptake will closely align the sector with the European Climate Law, the EU's strategy to comply with a 2°C pathway (Eamonn Mulholland J. M.-L., 2022). Comments are therefore also provided on how a faster transition to ZEVs for HDVs would influence the environmental and health impacts of tampering.

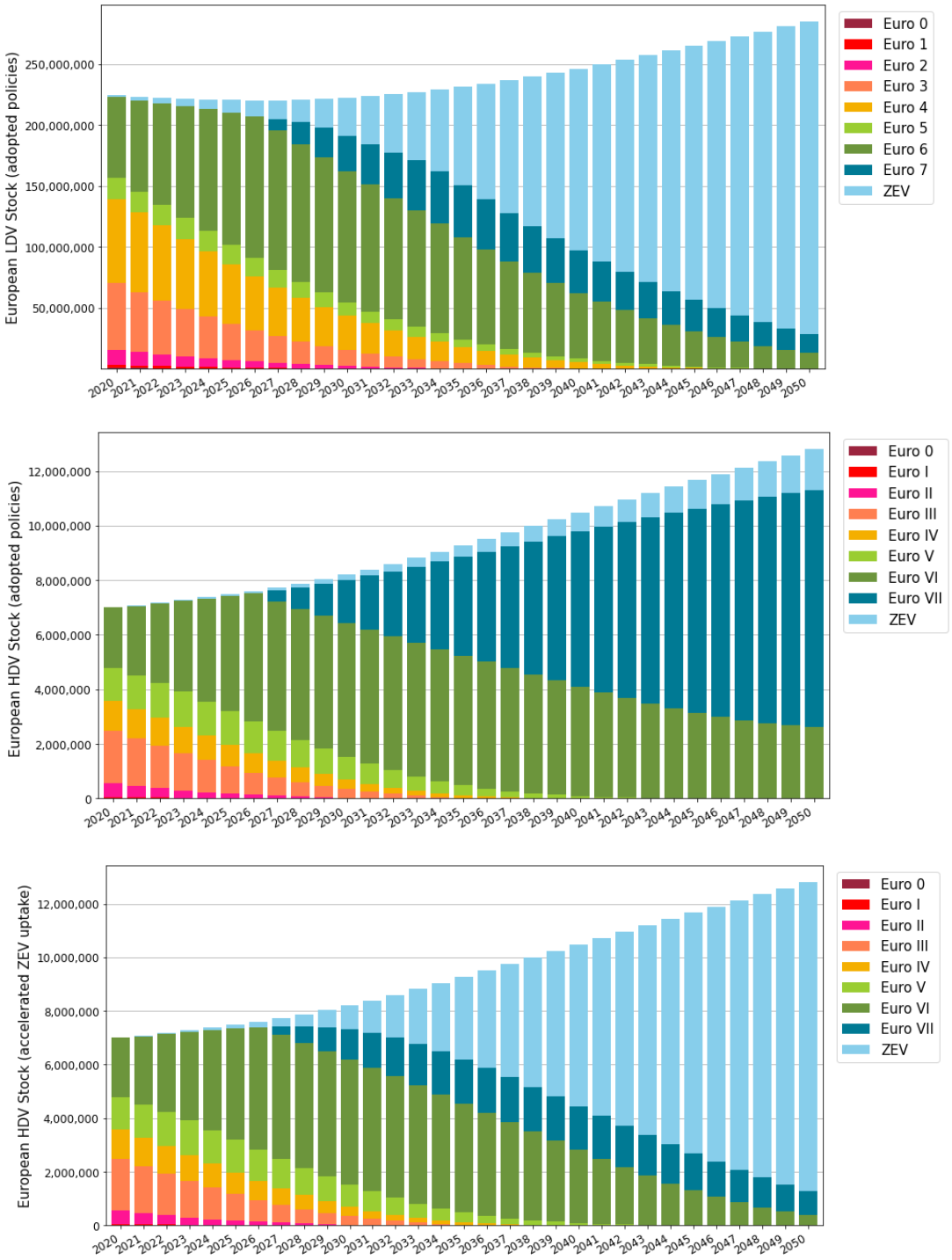


Figure 2-2: Projected stock of vehicles in the European fleet out to 2050, by emission control level, for light-duty vehicles (LDVs, top panel) and heavy-duty vehicles (HDVs, bottom two panels). The accelerated ZEV uptake case for heavy-duty vehicles considers the adoption of more stringent CO2 standards in line with the European Climate Law.

Roadmap models the real-world emissions of on-road vehicles. For each emissions control standard (e.g., Euro 5/V, Euro 6/VI, etc.), emission factors are therefore defined to account for applicable conformity

factors at type approval and for real-world deviations from the regulatory limits, as observed from remote sensing data. Emission factors for vehicles type-approved to standards up to Euro 6/VI are informed by the European Monitoring and Evaluation Program (EMEP) and the Handbook Emission Factors for Road Transport (HBEFA). For the upcoming Euro 7/VII standards, a regulatory proposal for the stringency of the pollutant emissions limits and for the standards implementation date is expected in October 2022. In the meantime, the assumed emission factors are informed by global regulatory developments, demonstration programs led by industry stakeholders, and assessments carried out by the European Commission's contractors. For light-duty vehicles, it is assumed that Euro 7 could achieve an 80% and 66% reduction in NOx emissions for diesel and gasoline vehicles, respectively, compared to Euro 6d vehicles. For heavy-duty vehicles, it is assumed that Euro VII could achieve a 79% reduction in NOx emissions compared to Euro VI-D/E vehicles (Eamonn Mulholland J. M., 2021).

2.1.3 Inputs to tampering modelling

Two parameters are used to determine the contribution of tampering to the total emissions and its impact on air quality and health issues, namely tampering shares and tampering rates.

2.1.3.1 Tampering shares

The share of tampered vehicles, hereafter referred to as "tampering share" (in % of the vehicle fleet), describes the incidence of tampering in the total vehicle fleet. It is defined for each vehicle type (passenger cars, trucks and buses) and emission control level (the so-called "Euro" standards) as the share of the vehicles being tampered with. Furthermore, based on the tampering case, different Environmental Protection Systems (EPS), and in turn types of pollutants, are affected. Thus, different tampering shares can be drawn for each type of pollutant.

Tampering shares are mostly extracted from remote sensing of real driving emissions campaigns and relative reports. To identify tampering via remote sensing, 2 basic steps are followed:

1. High-emitters identification: Specific tailpipe emissions thresholds are defined, above which the vehicle is identified as a high-emitter. Tailpipe emissions are measured via remote sensing techniques (i.e. cross-road snapshots, top-down snapshots, plume chasing, and point sampling).
2. Tampered high-emitters identification: A tampered high-emitter is identified via visual inspection and other tampering-related checks e.g.:
    - Visual inspection of the most common "attack points" on the vehicle wiring
    - Visual inspection for removed exhaust components
    - Visual inspection of AdBlue tank level compared to tank level in the dashboard
    - Checks of the resistance of the Controller Area Network (CAN) line
    - Checks via OBD testers for frequent Diagnostic Trouble Code (DTC) erasing

From steps 1 and 2, the high-emitters and the tampered high-emitters shares [%] can be respectively estimated. Regarding the tampered high-emitter share [%], Periodic Technical Inspections (PTI) may also provide input. In this case, the 1st step can be skipped since direct inspection for tampering devices is possible.

All available information was aggregated in Table 2-1. During the data research and collection, limitations regarding availability and comparability were encountered. To better understand these limitations and draw, where possible, some reasonable assumptions, discussions were initialized with the national or

independent authorities taking part in remote sensing campaigns (e.g. Danish police squad, Port of Antwerp), and synergies with relevant EU projects (e.g. CARES[2]) were exploited.

Limited data are available since only a few remote sensing reports provided results including both high-emitters and tampered high-emitters shares, while the vast majority of all data available refer to Euro V and Euro VI (not always separately classified) trucks considering tampering attacks that affect the NOx emissions. Additionally, data available correspond to different countries of vehicle registration.

The data comparability is mainly affected by the differences encountered in each campaign with respect to high-emitters and tampered high-emitters identification. Results regarding high-emitters identification depend on the emissions thresholds set and the technique used to measure tailpipe emissions. As reported on a recent remote sensing campaign in Berlin (Ingenieurbüro Lohmeyer GmbH & Co. KG, 2021), qualitatively, it is clear that at a very high threshold for a "conspicuous" emission rate (e.g. a multiple of the emission limit value) tends to require fewer measured values to identify a high-emitter. However, a very high threshold may also allow a number of vehicles with poorly adjusted exhaust gas cleaning to pass unnoticed.

Vehicle remote sensing technologies measure pollutant concentrations in a vehicle's exhaust plume without physical interaction with the vehicle, unlike portable emission measurement systems (PEMS). The measurement is succeeded via spectroscopy as the vehicle drives through a light beam (i.e. cross-road or top-down snapshots) or, alternatively, extracts a sample from the exhaust plume to measure with pollutant analyzers (i.e. plume chasing, and point sampling). The first method is less accurate resulting in more false-positive high-emitters (or higher thresholds must be set to consider measurement uncertainty), but it is also less time-consuming (~1" per measurement) meaning that more vehicles can be measured per day. Based on experience from plume chasing tests, CARES project partners stated that there is a trade-off between measurement duration and the definition of the right thresholds to identify high emitters. The longer you measure, the closer you come to EU official limits and lower variability in tailpipe (NOx) emissions is succeeded. In this sense, identifying high emitters via plume chasing or point sampling has an advantage compared to emissions snapshots. Nevertheless, to reach statistical confidence and robustly estimate the high-emitters vehicle share in the whole fleet, a critical amount of remote sensing data must be collected at different sites and under different conditions.

Considering the effectiveness of tampered high-emitters identification, some basic limitations are observed. In all tampering-related numbers used Engine Control Unit (ECU) flashing is excluded because ECU flashing is difficult to be identified via roadside inspections. A few roadside inspection officers from some EU members (i.e. Danish police squad) report using simple but intelligent methods to search for tampering via ECU flashing. Preliminary results from a relevant remote sensing campaign in Denmark on February 2022, estimate that 7.4% of the whole country's passenger cars fleet is tampered with by means of ECU flashing concerning Diesel Particulate Filter (DPF) and Exhaust Gas Recirculation (EGR) mainly. Visual inspections may also be ineffective in other cases. For example, some hardware emulators may not be found due to their small size. Furthermore, additional variability in results is introduced from the fact that not the same steps of visual inspection and strategy to identify tampering are followed in each campaign. For instance, as stated by CARES partners, Denmark inspections in 2020 sought mainly NOx-related defects or manipulations on HDV. Also, if a defect was avoided and "hidden" through emulators

[2] https://cares-project.eu/

or other means (i.e. repeated deletion of DTCs), authorities were classifying this case as a defect, not tampering.

Table 2-1: Tampering shares (%)

Country	Vehicle type	Vehicle registration	Euro 5/V			Euro 6/VI			Total (Euro 5/V + Euro 6/VI)			EPS (/pollutant) affected	Reference
			High emitters	Tampered high emitters	Tampering share	High emitters	Tampered high emitters	Tampering share	High emitters	Tampered high emitters	Tampering share		
Austria	**Trucks**	**All countries**	-	-	-	-	-	-	10%	**15%**	1.5%	SCR (NOx)	(Buhigas, De la Fuente, & Montero, 2019)
Austria	**Trucks**	**Mostly East/South Europe**	**35%**	50%	17.5%	**25%**	50%	12.5%	-	-	-	SCR (NOx)	(Pöhler, et al., 2019)
Sweden	**Trucks**	**All countries**	-	-	-	**2%**	50%	1%	-	-	-	SCR (NOx)	(Jerksjö, 2019)
Germany	**Trucks**	**Germany**	-	-	-	**6.9%**	50%	~3.5%	-	-	-	SCR (NOx)	(Pöhler & Adler, 2016)
Germany	**Trucks**	**Eastern Europe**	**~26%**	50%	~13%	**18.9%**	50%	9.5%	-	-	-	SCR (NOx)	(Pöhler & Adler, 2016)
Spain	**Trucks**	**All countries**	**20%**	**47%**	**9.4%**	-	-	-	-	-	-	SCR (NOx)	(Buhigas, De la Fuente, & Montero, 2019)
Denmark	**Trucks**	**All countries**	**6.2%**	**20%**	**~1.2%**	**2.2%**	**27%**	**~0.6%**	**3.4%**	**24%**	**~0.8%**	SCR (NOx)	(Ellermann, Hertel, Winther, Nielsen, & Ingvardsen, 2018)
Switzerland	**Trucks**	**All countries**	-	-	-	-	-	-	-	-	**~1%**	SCR (NOx)	(UNECE, 2018)
UK	**Trucks**	**All countries**	-	-	-	-	-	-	-	-	**~4%**	SCR (NOx)	(Harris, 2018)
UK	**Lorries**	**UK**	-	-	-	-	-	-	-	-	**8%**	DPF, SCR, EGR (PM/PN, NOx)	(AECC, 2018)
Germany	**Taxis**	**Germany**	-	-	-	-	-	-	-	-	**10%**	DPF (PM/PN)	(Pauwels, 2017)
Germany	**Passenger cars**	**Germany**	-	-	-	-	-	-	**10%**	50%	5%	DPF, EGR (PM/PN, NOx)	(Thürmer & Schuster, 2018)
Netherlands	**Passenger cars**	**Netherlands**	**12.5%**	50%	~6%	**5%**	50%	2.5%	**6%**	50%	3%	DPF (PM/PN)	(Laenen, 2020)
EU fleet	**Passenger cars**	**All countries**	-	-	-	-	-	-	-	-	**4%**	DPF (PM/PN)	(Pauwels, 2017)

Notes: Inputs from remote sensing reports are in bold, while assumed inputs have normal font. Tampering share is the product of high emitters and tampered high emitters shares. Assumptions were made based on the max known shares.

2.1.3.2 Tampering rates

Tampering rate is defined as the ratio between the emission level of a tampered vehicle and the emission level of a vehicle with a functional emission control system, the latter being informed by the emission factors described in section 2.1.2. Tampering rates are also defined for each vehicle type and emission control level, as well as for different pollutant types.

Tampering rates reflect the most common type of tampering and the part of the emissions control system that is targeted in each case. For example, in Euro VI-certified trucks, the most common type of tampering is to deactivate urea injection to the selective catalytic reduction (SCR) and the associated tampering rate therefore expresses this as an increase in NO_x emissions. In general, NOx-inducing tampering is associated with tampering with the SCR system for diesel vehicles and tampering with the three-way catalyst (TWC) for gasoline vehicles. PM-inducing tampering is associated with tampering with the diesel particulate filter (DPF) for diesel vehicles and tampering with the gasoline particulate filter (GPF) for gasoline vehicles. Particulate matter is characterized by both particulate mass and particulate number, both of which are regulated separately in pollutant emission standards. However, this study defines tampering rates for particulate mass only.

Tampering emission rates can be estimated based on:

a) Test results from tailpipe emissions from tampered vehicles in chassis dyno or on the road (remote sensing, plume chasing, PEMS, Smart Emission Measurement System (SEMS)) compared with non-tampered data from the same vehicle
b) Test results from engine-out emissions of non-tampered vehicles compared with tailpipe emissions (assuming full tampering)
c) Emission data for the same engine in current and previous registrations without an EPS

Since tampering does not necessarily lead to engine-out emissions (e.g. SCR but not EGR deactivation, partly deactivated SCR, etc.), in the current analysis, the (a) test results were used to extract the tampering rates. Data were available from remote sensing reports or relevant publications, as well as from previous DIAS deliverables. Collected data (Table 2-2) have a great degree of variability since the effect on tailpipe emissions varies depending on the tampering attack. Thus, most reports give a range and not an exact value of the tampering rate. For example, Vermeulen et al. (Vermeulen, Verbeek, & van Goethem, 2017) report that the deactivation of the SCR can increase NOx for Euro V trucks from a factor of 2-4, while for a Euro VI truck this increase could add up to a factor 12 on average, and up to a factor 20 if for instance the EGR is manipulated as well.

Table 2-2: Tampering rates

Pollutant	Vehicle type(s) and fuel	Tampering rate				Reference
		Euro 5/V	Euro VI/6	Euro 5/V + Euro 6/VI	Undefined	
NOx	**Trucks**	2-4	10			(Buhigas, De la Fuente, & Montero, 2019)
NOx	**City buses**	3-20	-	-	-	(MODALES, 2021)
NOx	**Trucks**	2-4	12 (average), <20	-	-	(Vermeulen, Verbeek, & van Goethem, 2017)
NOx	**Trucks**	-	7-16	-	-	(uCARe, 2019)

NOx	**Trucks**	-	2-33	-	-	(Jerksjö, 2019)
NOx	**Trucks**	-	-	-	<45	(Denmark Ministry of Transport, 2018)
NOx	**HDVs**	-	4-20	-	-	(uCARe, 2019)
NOx	**Trucks**	-	4-65	-	-	(D3.2, 2020)
PM	**Diesel LDVs and HDVs**	-	-	10	-	(Vojtíšek, Skácel, Beránek, & Pechout, 2018)
PN	**Diesel LDVs and HDVs**	-	-	>100	-	(Vojtíšek, Skácel, Beránek, & Pechout, 2018)
PN	**Diesel Passenger cars**	85-110	-	-	-	(Buekenhoudt, De Meyer, & Chavatte, 2019)
PN	**All equipped with DPF or GPF**	-	-	100-1000	-	(uCARe, 2019)

So far, research in the context of the DIAS project has shown that tampering mainly affects negatively NOx, PM, and Particulate Number (PN) emissions. Regarding tampering rates and shares for other pollutants [e.g. Carbon monoxide (CO), Methane (CH_4), Total hydrocarbons (THC), Ammonia (NH_3), Nitrous oxide (N_2O), NO_2], no further data or robust assumptions based on expert guesses were available. It should be noted that tampering may have a positive effect on emissions in this case. For example, SCR removal can lead to lower NH_3 and N_2O emissions while if Diesel Oxidation Catalyst (DOC) is removed NO_2 emissions are expected to be reduced.

Tampering is only modelled in vehicles certified with emission control levels starting from Euro 5/V, due to scarce data for older vehicles. As shown in Figure 2-2, older vehicles will still represent a significant portion of the fleet well after 2030. However, for those older vehicles, the impact of tampering is expected to be less important, as emission control systems have lower conversion rates and tailpipe emissions in non-tampered vehicles are therefore closer to the engine-out values exhibited by tampered vehicles.

For vehicles certified with emission standards starting from Euro 5/V, due to the limited amount of data presented above, scenarios were developed to assess the real-world emissions and health impacts of tampering.

2.1.4 Modelling Scenarios

Three different scenarios were developed to cover a wide range of tampering incidence and tampering rates from the data presented in the previous section. Additionally, to quantify the potential benefits of introducing anti-tampering regulation, one additional scenario considered the case in which there is no tampering at all. Following are the four different scenarios being investigated:

Scenario 1: Counterfactual scenario

This scenario assumes no tampering occurred historically or will occur in the future. This counterfactual scenario is used as a baseline for calculating the effects of tampering. Because it assumes no tampering, it also illustrates the maximum theoretical benefits of anti-tampering regulation.

Scenario 2: Central Estimate scenario

This scenario reflects our best estimate for the actual tampering shares and tampering rates based on evidence from different roadside inspections and remote sensing emission measurement campaigns in Europe.

Scenario 3: Worst-Case scenario

This scenario models the highest values of tampering shares and tampering rates from the available data, which reflects a worst-case scenario and provides an upper bound for the real-world impacts of tampering.

Scenario 4: Best-Case scenario

This scenario models the lowest values of tampering shares and tampering rates from the available data, which provides a lower bound for the real-world impacts of tampering.

The tampering shares and tampering rates used in each scenario are summarized in Table 2-3 and Table 2-4.

Table 2-3: Share (in %) of the tampered vehicles in the European fleet by vehicle type, Euro standard and pollutant, for the four modelling scenarios.

Vehicle Type	Scenario	NOx			PM		
		Euro 5/V	Euro 6/VI	Euro 7/VII	Euro 5/V	Euro 6/VI	Euro 7/VII
Light-duty vehicles - gasoline	Counterfactual	0	0	0	0	0	0
	Central Estimate	0	0	0	0	2.5	1.3
	Worst-Case	0	0	0	0	5	2.5
	Best-Case	0	0	0	0	1.3	0.7
Light-duty vehicles - diesel	Counterfactual	0	0	0	0	0	0
	Central Estimate	2.5	5	2.5	5	5	2.5
	Worst-Case	10	10	5	10	10	5
	Best-Case	2.5	2.5	1.3	2.5	2.5	1.3
Heavy-duty vehicles	Counterfactual	0	0	0	0	0	0
	Central Estimate	8.6	6	3	8.6	6	3
	Worst-Case	18	13	6.5	10	10	5
	Best-Case	2.5	2.5	1.3	2.5	2.5	1.3

Table 2-4: Tampering rates, defined as the ratio of tampered to non-tampered vehicle emissions, by vehicle type, Euro standard and pollutant, for the four modelling scenarios.

Vehicle Type	Scenario	NOx			PM		
		Euro 5/V	Euro 6/VI	Euro 7/VII	Euro 5/V	Euro 6/VI	Euro 7/VII
Light-duty vehicles - gasoline	Counterfactual	1	1	1	1	1	1
	Central Estimate	1	1	1	1	5	25
	Worst-Case	1	1	1	1	5	25
	Best-Case	1	1	1	1	2.5	25
	Counterfactual	1	1	1	1	1	1

Light duty vehicles - diesel	Central Estimate	4	10	20	10	10	50
	Worst-Case	4	10	20	10	10	50
	Best-Case	4	10	20	10	10	50
Heavy-duty vehicles	Counterfactual	1	1	1	1	1	1
	Central Estimate	4	10	20	4	10	50
	Worst-Case	4	20	40	4	10	50
	Best-Case	4	10	20	4	10	50

Regarding Euro 5 and 6 gasoline passenger cars, negligible (or zero) TWC-related (and thus NOx-related) tampering attacks were observed while no tampering is expected for Euro 7 vehicles. During DIAS research, it was shown that TWC-related tampering was an issue in older (i.e. Euro 4) vehicles which had higher rates of malfunctions and thus tampering motivation. Furthermore, for Euro 5 gasoline cars, there is no PM/PN-related EPS and thus no tampering impact can be expected.

The Euro 5/V NOx tampering rate is assumed lower than the Euro 6/VI NOx tampering rate since, in Euro 5/V vehicles, only EGR tampering affects NOx emissions. Euro 6/VI diesel vehicles, on the other hand, are also affected by SCR tampering. Similarly, the PM tampering rate for Euro 5/V vehicles is assumed lower than for Euro 6/VI PM rate because the PM-related EPS used in Euro 6/VII DPF technology is much more effective in reducing PM/PN (i.e. >99%) than the Continuous Regenerating Trap (CRT) used in Euro 5/V DPF technology.

The tampering shares used in the Central Estimate scenario represent a weighted average of the individual samples (samples regarding all countries are affected by weight of either 1 or 0.5) and realistic estimations from experts (regarding LDVs). For the Worst-Case and Best-Case scenarios, higher or lower values were chosen, respectively. The PM tampering shares used in the Worst-Case scenario for PM in HDVs are assumed lower than for NOx since, for HDVs, NOx-related tampering (either by means of emulators installation or ECU flashing) results in higher financial benefits by mitigating or totally avoiding Adblue consumption. For this reason, remote sensing campaigns measuring commercial vehicles mainly targeted NOx high-emitters. As shown in Table 2-1, the only available input for PM tampering shares on HDVs was from a report from the Association for Emissions Control by Catalyst (AECC) in the UK concluding in an 8% share of lorries tampered with both NOx and PM-related EPS (AECC, 2018). Therefore, for the remaining scenarios, the same tampering share was assumed for NOx and PM.

The tampering shares and rates used for Gasoline passenger cars are lower than the diesel ones since Gasoline Particle Filters (GPFs) are less prone to failure and have lower needs for replacement (thus less motivation for tampering) than diesel exhaust control systems. This is explained by several factors. First, there is extensive knowledge of GPFs compared to DPFs that have been introduced more recently. Second, due to the lower soot load in the GPF, the exotherm during regeneration is lower compared to diesel systems, resulting in less uncontrolled regenerations. Even for future actively regenerated systems (e.g. hybrids with no fuel cut-offs), the regeneration strategy can be controlled (e.g. spark retard and air-fuel-ratio modulation). In general, the soot combustion rate and the exotherm can be easily controlled by metering the oxygen flow into the GPF. However, increasing occurrences of tampering in GPFs may be observed in future years, because the number of GPF applications has increased rapidly after 2017. GPF tampering therefore only applies to EU6d-TEMP and later vehicles.

While for diesel light-duty vehicles taxis are the main vehicle use case affected by tampering, there is a low number of gasoline taxis, thus lower GPF tampering shares are assumed (50% compared to diesel vehicles). PN/PM gasoline emissions are mainly observed during cold start, whereas in diesel vehicles they occur in all operating conditions. Additionally, the efficiency of GPFs is lower than that of DPFs. Therefore, 50% lower emission rates are assumed compared to diesel vehicles.

Assuming that stringent Euro 7/VII emission limits will lead to higher efficiency of the aftertreatment system in non-tampered vehicles (e.g. higher efficiency of the SCR at 99.5% and NOx levels required to drop below 30 mg/km), tampering rates are assumed to be higher than in Euro 6/VI vehicles. NOx tampering rates are assumed to be twice as high for NOx (in both LDVs and HDVs) and five times as high for PM (in HDVs). Tampering shares for Euro 7/VII vehicles were assumed as half of the Euro 6/VI ones, assuming a partial elimination of tampering due to near-future emissions monitoring components of the legislation, such as On-Board Monitoring (OBM).

For non-tampered vehicles, an emission factor of 1 is assumed, meaning that a vehicle's emissions are exactly at the level of the regulatory limit. While in practice a deviation from the limit is allowed, this simplifying assumption is made to isolate the impact of tampering more easily.

Based on the defined tampering rates for the Central Estimate scenario, the emissions produced by every tampered Euro 6/VI vehicle are equivalent to those produced by 23 and 27 non-tampered vehicles in terms of NO_x and PM emissions in the year 2030, respectively. For Euro 7/VII vehicles, the emissions produced by every tampered vehicle are equivalent to those produced by 47 and 107 non-tampered vehicles in terms of NO_x and PM emissions, respectively.

Figure 2-3 shows the number of vehicles with NOx and PM inducing tampering in the European fleet in 2022, resulting from the defined tampering shares in each modelling scenario. In some tampered vehicles, both the NOx-controlling and PM-controlling systems are tampered with. However, this is not always the case. The Central Estimate scenario therefore results in between 4 and 6 million tampered vehicles in 2022, depending on the extent of the overlap between both types of tampering. Similarly, the Worst-Case scenario results in between 7 and 12 million tampered vehicles, and the Best-Case scenario results in between 2 and 3 million tampered vehicles.

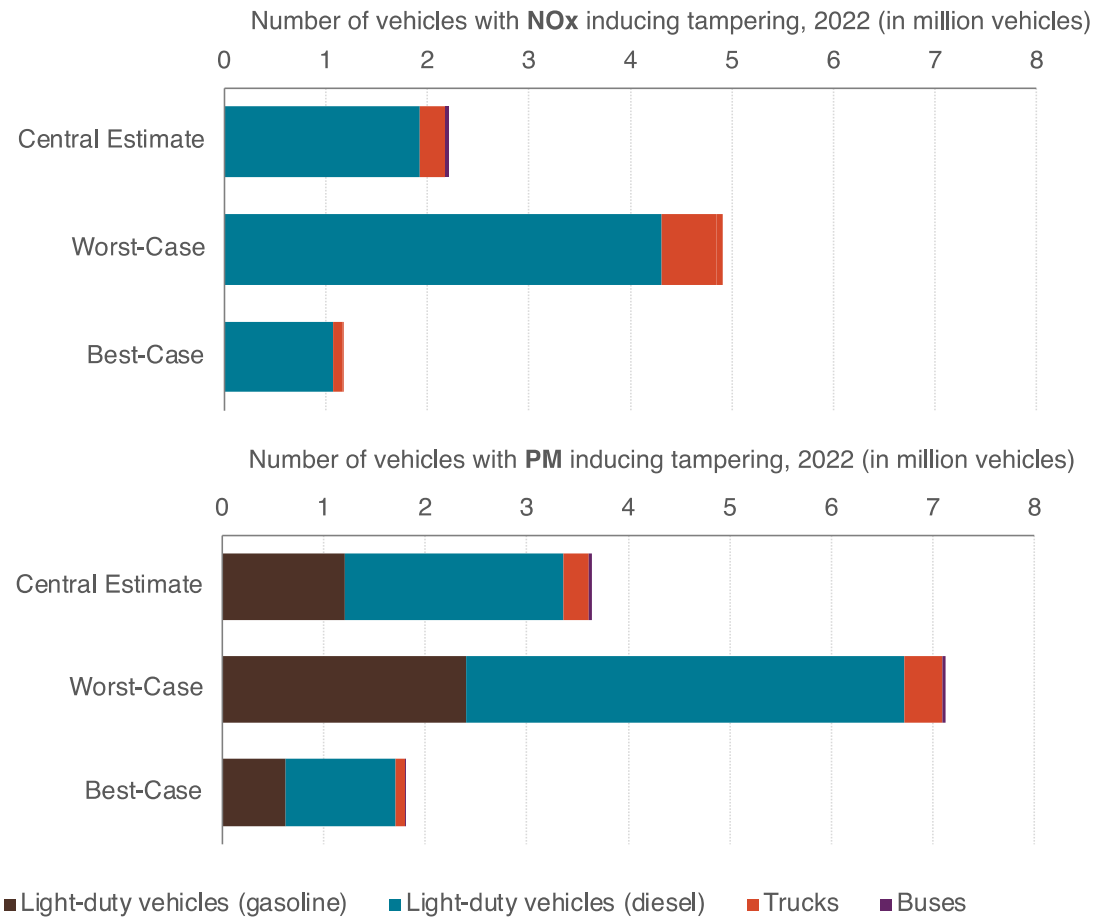


Figure 2-3: Number of vehicles with NOx (top) and PM (bottom) inducing tampering in the European fleet in 2022 under each modelling scenario, by vehicle type. Some overlap exists between vehicles with both types of tampering.

Figure 2-4 shows the evolution with time of the tampered vehicle stock, broken down by emissions control level, for the Central Estimate scenario. The share of vehicles certified with different emissions standards in the tampered vehicle fleet is the same across all scenarios; only the total number of tampered vehicles varies, according to Figure 2-3**.**

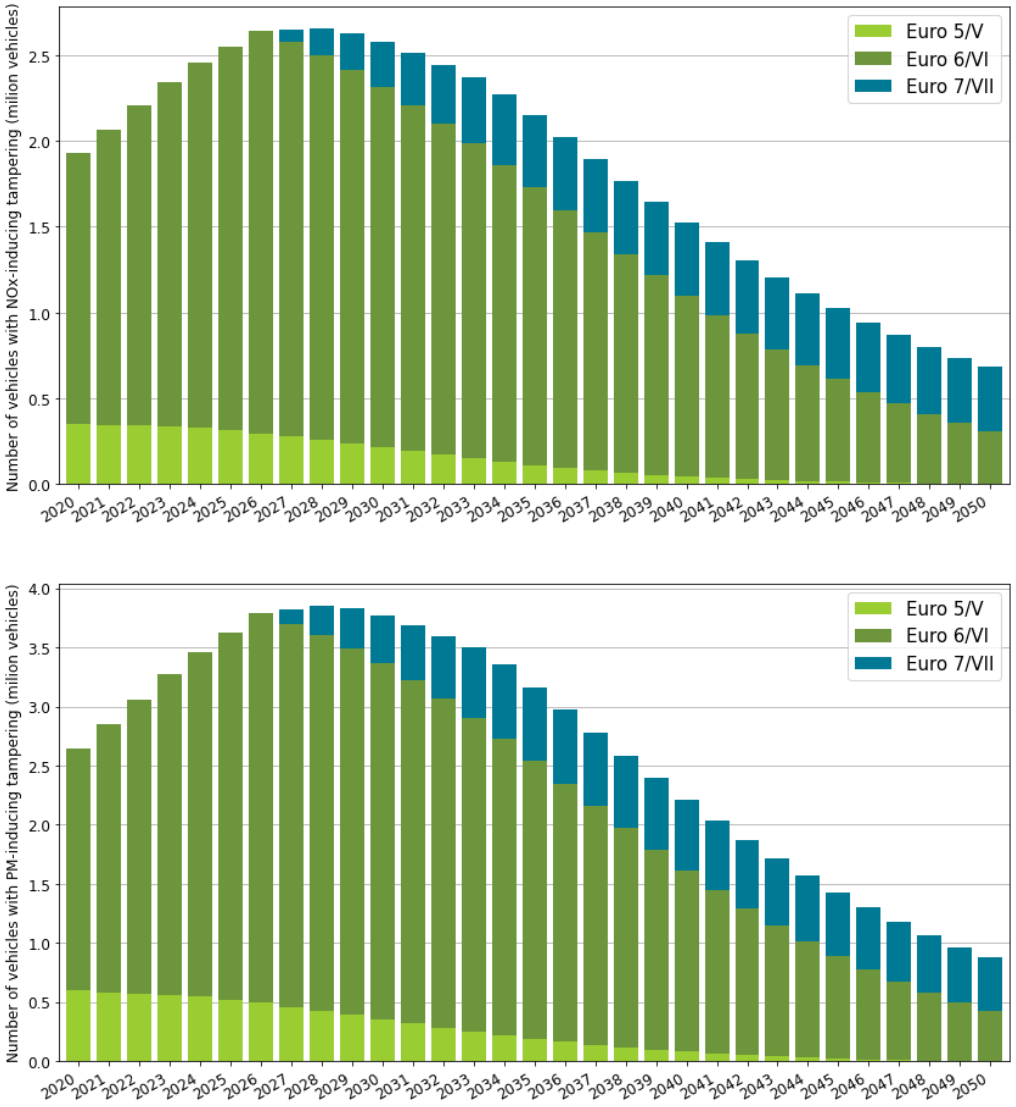


Figure 2-4: Share of each emission standard in the stock of vehicles with NOx (top) and PM (bottom) inducting tampering out to 2050 under the Central Estimate scenario. The breakdown by emission standard is the same in all modelling scenarios.

The number of tampered vehicles is expected to increase out to 2028 as more Euro 6/VI vehicles are introduced to the fleet, and Euro 6 certified passenger cars have a higher tampering share than their Euro 5 counterparts (see Table 2-3). However, in the following years, the increasing share of zero-emission vehicles, and the introduction of Euro 7/VII vehicles that are less prompt to tampering, leads to a decrease in the number of tampered vehicles. By 2050, about the same number of tampered vehicles are expected as in 2022. Euro 6/VI vehicles represent the majority of tampered vehicles through 2050.

The following sections explore the impact this tampered vehicle fleet has on pollutant emissions and air quality-related health issues.

2.2 Environmental impact

This section presents the results of the emissions modelling with the Roadmap model (first modelling stage according to Figure 2-1). Figure 2-5 and Figure 2-6 show total fleet emissions of NOx and PM, attributable to different emissions control levels under all modelling scenarios. Total NOx and PM emissions from the on-road fleet are modelled to reduce with time, as older vehicles are replaced either with vehicles certified to stricter emission standards – Euro 6/VI out to 2027, then Euro 7/VII – or with zero-emission vehicles. Under the Central Estimate scenario, NOx emissions reduce 52% by 2030, 84% by 2040, and 93% by 2050. In the same time frame, PM emissions reduce by 62%, 89% and 94%, respectively.

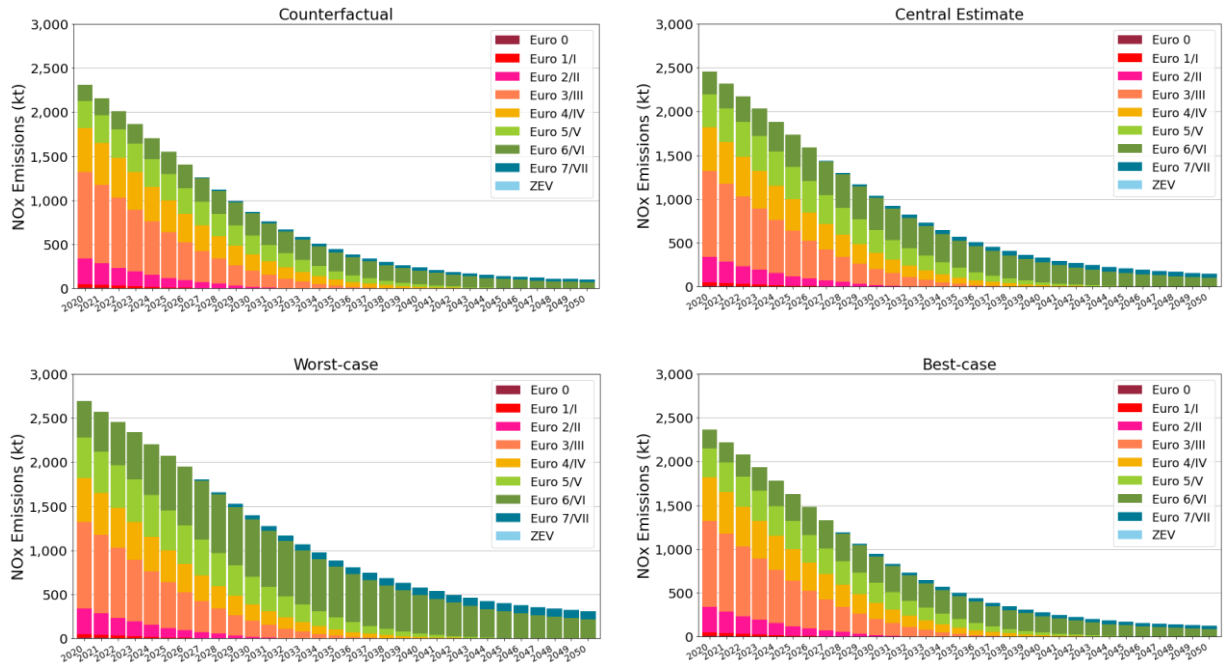
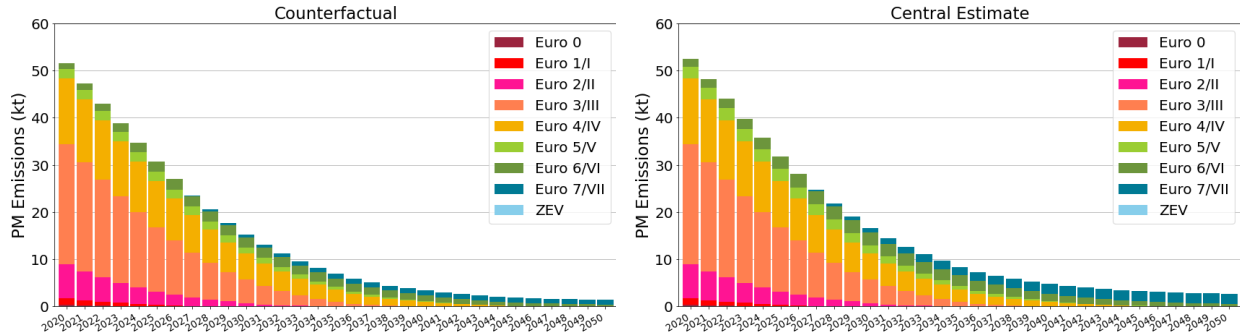


Figure 2-5: Total fleet NOx emissions, by emission control level, under each modelling scenario.



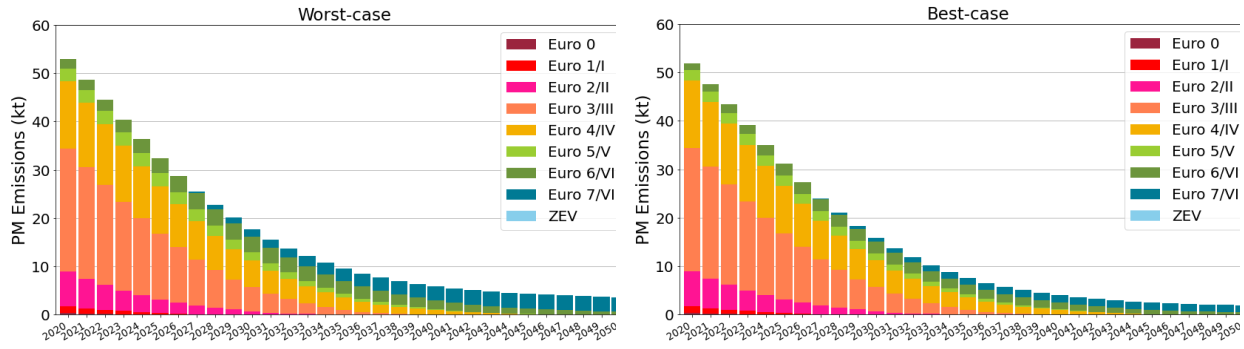


Figure 2-6: Total fleet PM emissions, by emission control level, under each modelling scenario.

Figure 2-7 shows the breakdown of the total fleet emissions of NOx and PM in 2022 by vehicle type (light-duty gasoline, light-duty diesel trucks and buses). The share by vehicle type varies within 1% across all modelling scenarios, hence only results for the Central Estimate scenario are presented. Despite representing only around 4% of the vehicle fleet – and 15% of the vehicle kilometres travelled, HDVs (trucks and buses) account for 66% of NOx emissions, and 45% of PM emissions in 2022 in all scenarios. The main reason for this disproportionate share of HDV emissions is their higher energy consumption – the average HDV in 2022 consumes 350 kWh/km, while the average LDV consumes 55 kWh/km. As a faster uptake of zero-emission vehicles is modelled for LDVs than for HDVs, the share of emissions attributable to HDVs is projected to further increase with time, reaching 80% for NO_x emissions and 68% for PM emissions in 2050. However, in the case of an accelerated ZEV uptake for HDVs, their contribution to total NOx and PM emissions would reduce to 37% and 19% in 2050, respectively.

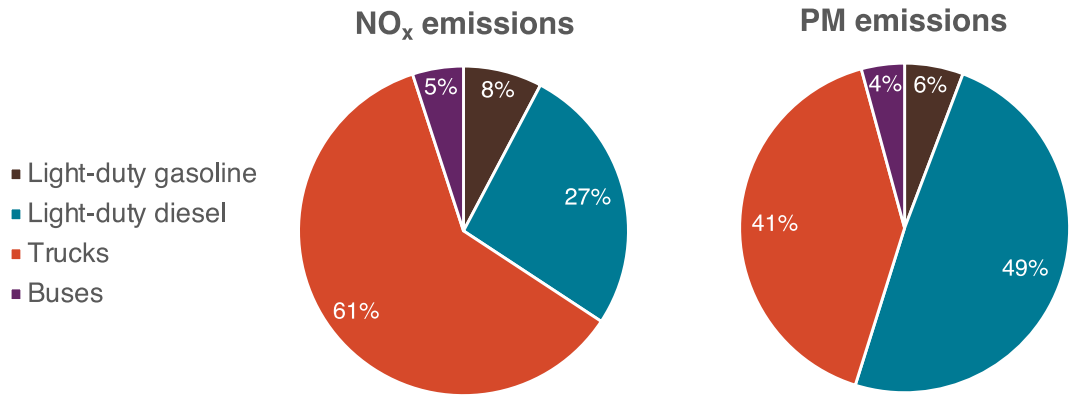


Figure 2-7: Share of total NOx and PM emissions attributable to different vehicle types in 2022, under the Central Estimate scenario. The share by vehicle types varies within 1% across all scenarios.

Tampering is found to significantly increase emissions in both light-duty and heavy-duty vehicles. Figure 2-8 shows the projected cumulative NOx emissions over the 2022-2050 period for all modelling scenarios considered, identifies excess emissions due to tampering, and shows the breakdown of those excess emissions by vehicle emissions standard. Figure 2-9 does the same for PM emissions. This study only models tampering in gasoline and diesel vehicles, therefore the percentages of excess emissions due to tampering are relative to the emissions from gasoline and diesel vehicles only.

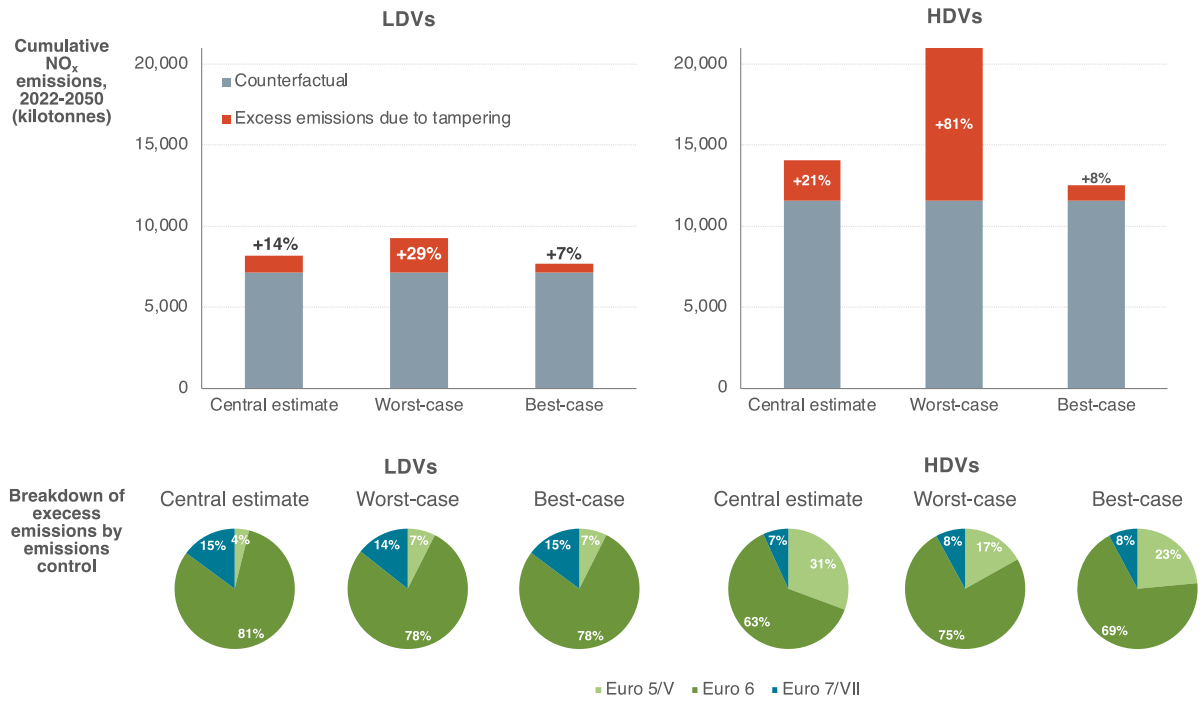


Figure 2-8: Cumulative NOx emissions over the 2022-2050 period, share attributable to tampering, and breakdown by emission standard, under all modelling scenarios.

Tampering is estimated to increase NOx emissions in LDVs between 7% and 29% over the 2022-2050 period depending on the modelling scenario, and 14% under the Central Estimate scenario. Under that scenario, 81% of excess emissions come from Euro 6 vehicles, 15% from Euro 7 vehicles, and 4% from Euro 5 vehicles. For HDVs, tampering is projected to increase NOx emissions between 8% and 81% over the 2022-2050 period, and 21% under the Central Estimate scenario. Excess emissions in that scenario originate at 63% from Euro VI vehicles, 31% from Euro V vehicles and 7% from Euro VII vehicles.

PM emissions from the European on-road vehicle fleet are projected to be less affected by tampering than NOx emissions, especially for heavy-duty vehicles. For light-duty vehicles, tampering is estimated to increase PM emissions by 6% over the 2022-2050 period under the Central Estimate, and up to 12% in the Worst-Case scenario. In the Central Estimate scenario, excess emissions originate mostly from Euro 7 (47%), Euro 6 (46%) vehicles, and to a minor extent from Euro 5 vehicles (7%). PM emissions from heavy-duty vehicles are projected to increase by 20% due to tampering in the Central Estimate scenario, and up to 32% in the Worst-Case scenario. For HDVs, most of the excess emissions come from Euro VII vehicles (58% under the Central Estimate scenario), followed by Euro VI (23%) and Euro V (19%) vehicles.

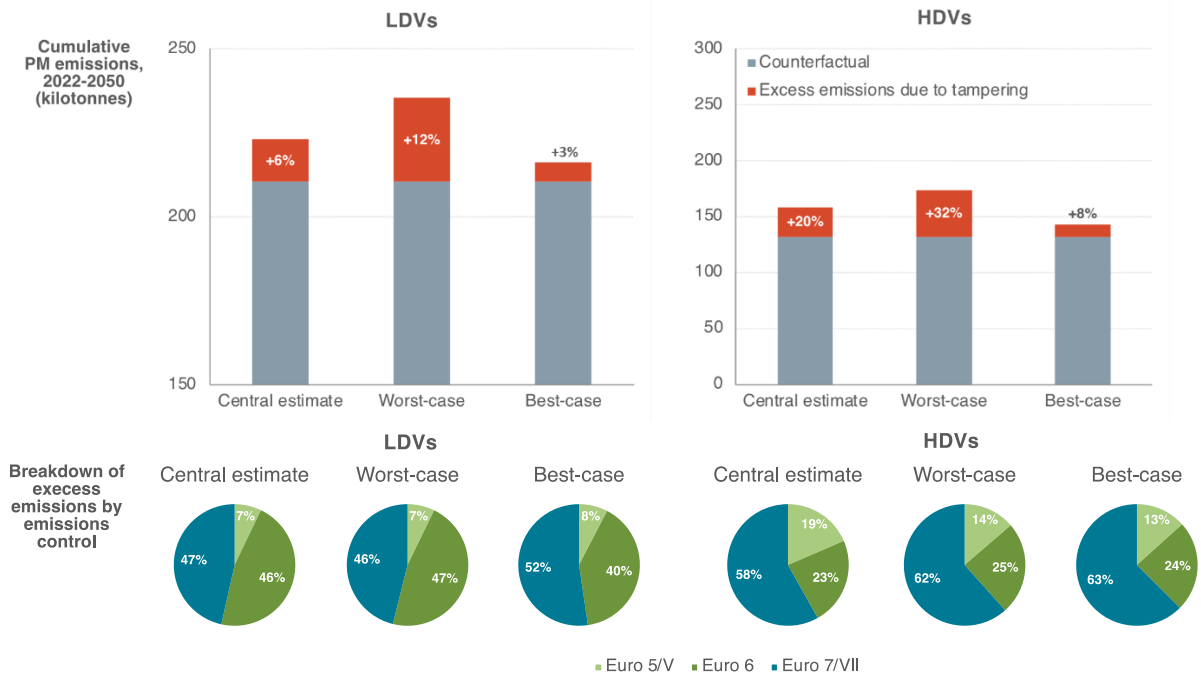


Figure 2-9: Cumulative PM emissions over the 2022-2050 period, share attributable to tampering, and breakdown by emission standard, under all modelling scenarios.

In the case of a faster zero-emission vehicle uptake for HDVs, the excess NOx and PM emissions due to tampering are expected to reduce to 19% and 11% over the 2022-2050 period, respectively, under the Central Estimate scenario. Faster uptake of zero-emission HDVs can therefore help mitigate the environmental impacts of tampering.

2.3 Health impact

Excess emissions from tampering result in higher ambient concentrations of harmful pollutants such as $PM_{2.5}$ and O_3. Long-term exposure to those pollutants can lead to several respiratory and heart-related diseases, which can eventually lead to air-quality-related premature deaths. Examples of causes of such premature deaths include stroke, ischemic heart disease, chronic obstructive pulmonary disease, lower respiratory infection, lung cancer, and diabetes mellitus type 2.

Based on the emissions modelling presented in the previous section, the health burden associated with tampering was determined with the FATE model. The number of premature deaths due to tampering, and the associated number of years of life lost arising from those premature deaths are determined for each modelling scenario. FATE models ambient pollutant concentrations resulting from various emissions sources, including non-transport-related sources. Therefore, to assess the health impacts of tampering, both health metrics are assessed for the different scenarios as compared to the Counterfactual scenario, in which no tampering is assumed.

Figure 2-10 shows the increase in the cumulative number of premature deaths and years of life lost throughout the years 2022 to 2050 incurred by tampering, for the different scenarios. Under the Central Estimate scenario, tampering leads to around 26,000 additional premature deaths, which equates to 464,000 years of life lost compared to a case of no tampering. This number increases to 82,000 premature

deaths which equates to 1,438,000 years of life lost under the Worst-Case scenario and decreases to 11,300 premature deaths and 198,000 years of life lost under the Best-Case scenario.

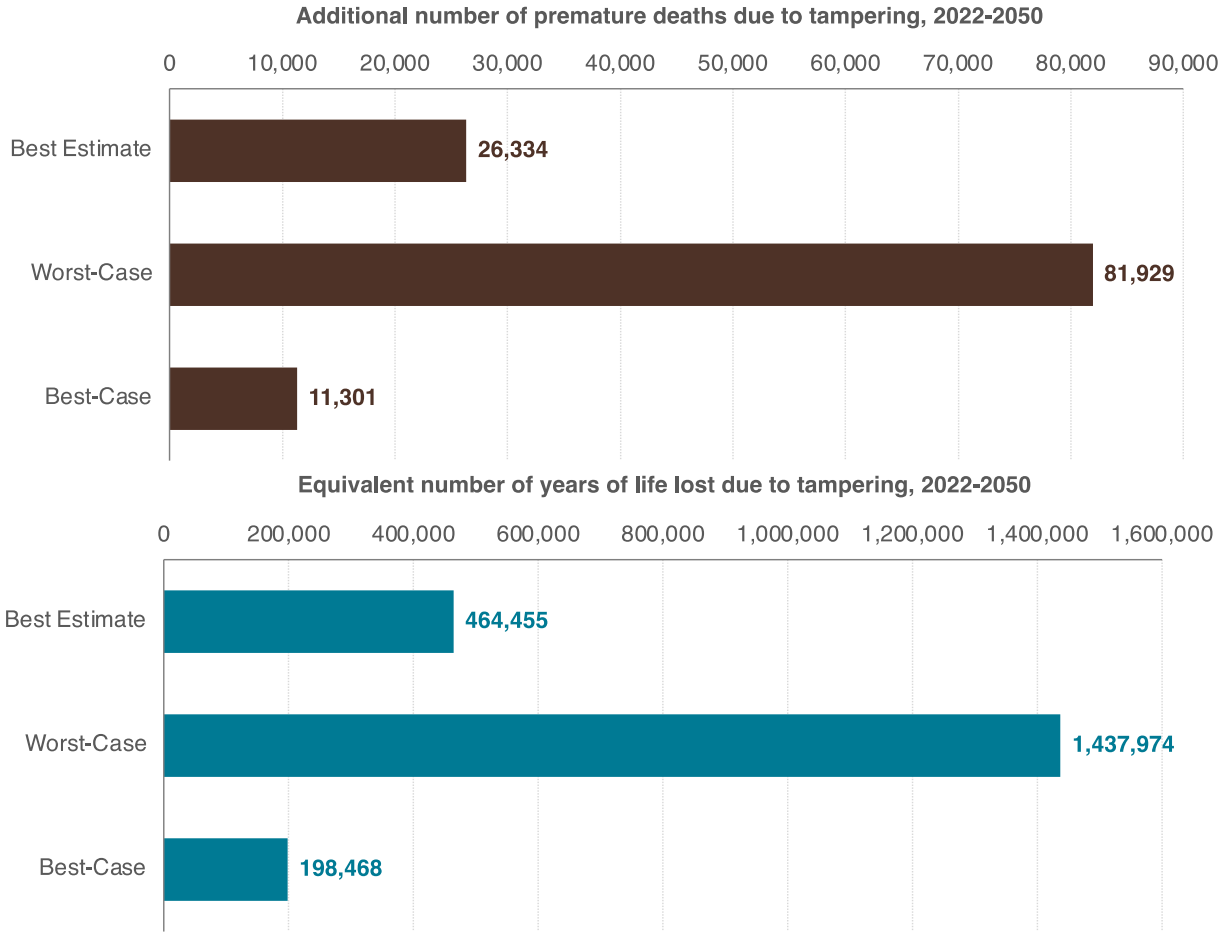


Figure 2-10: Additional cumulative number of premature deaths (top) and equivalent number of years of life lost (bottom) over the 2022-2050 period resulting from tampering-incurred emissions.

If heavy-duty vehicles were to experience an accelerated transition to zero-emission vehicles (as per Figure 2-2), the health burden associated with road transport emissions over the 2022-2050 period would reduce to 21,000 premature deaths and 378,000 years of life lost between under the Central Estimate scenario – that is, reductions in the health burden of 20% for premature deaths and 18% for years of life lost, compared to the case of a slower ZEV transition.

Figure 2-11 further shows the evolution out to 2050 of the number of premature deaths and the resulting number of years of life lost in each scenario relative to the Counterfactual scenario. In all cases, the health burden associated with tampering is expected to increase until around 2030, as more Euro 6/VI vehicles are introduced to the fleet, and those vehicles are responsible for most of the excess emissions from tampering, as shown in *Figure* 2-8 and *Figure* 2-9. As of 2030, tampering is projected to be responsible for additional 1,150 premature deaths and 21,000 additional years of life lost in the Central Estimate scenario. In the Worst-Case scenario, tampering leads to additional 3,500 premature deaths and a resulting 64,000 additional years of life lost in 2030.

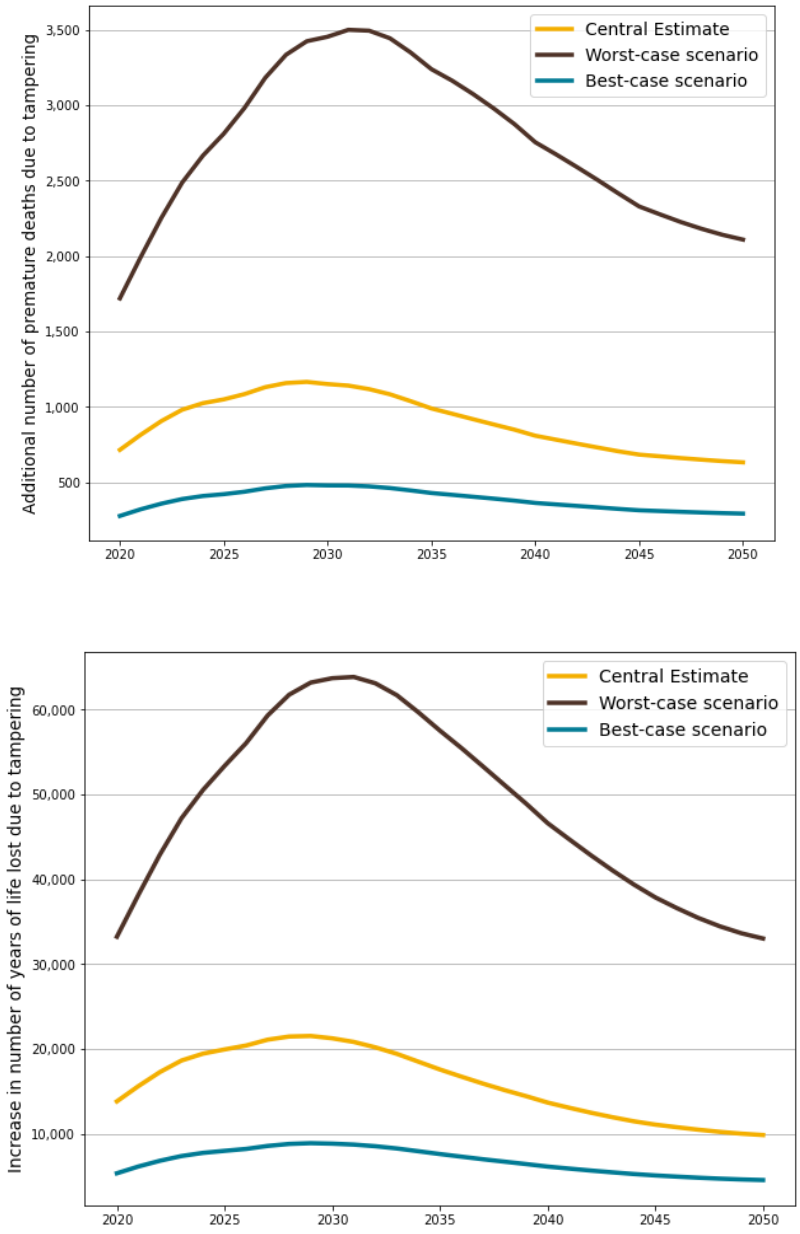


Figure 2-11: Difference in number of premature deaths (top) and resulting years of life lost (bottom) between the three scenarios modelling different levels of tampering and the counterfactual scenario, over the 2020-2050 period.

In the 2022-2030 period, the health burden increases much faster under the Worst-Case scenario than under the other two scenarios, highlighting the interest in limiting the extent of tampering to a minimum. After 2028, the health impacts of tampering are expected to reduce as excess emissions from tampering reduce, due to both the implementation of Euro 7/VII standards and a higher share of zero-emission vehicles. Still, it is projected that the health burden incurred by tampering in 2050 will remain around the same level as it currently is, both in terms of premature deaths and years of life lost. Tampering is therefore expected to remain a significant issue out to 2050.

2.4 Monetary impact

The monetary impact of tampering expresses the difference between the health (and environmental) burden expressed in monetary terms and the costs of the development and implementation of the anti-tampering measures. While there are means (e.g. relevant handbooks) to assess the first parameter, the second one is significantly more demanding.

In the context of DIAS, several technical solutions were identified addressing tampering detection (by monitoring and plausibilization of EPS-relate signals), prevention (by securing flashing process, SW execution, key management, and data exchange, and applying intrusion detection system and firewall) and reporting (by providing options for reporting scheme, infrastructure and tampering-related compliance certification). Estimations regarding the initial and operational cost and other aspects (more in section 4.2.2.3) of the solutions were attempted in (D2.3, 2022) but, in agreement with the whole DIAS consortium, this was finally possible only in binary-like qualitative terms. Furthermore, some solutions were not demonstrated within DIAS but only the main concept was documented and, occasionally, there was a strong dependency on new infrastructures not fully integrated into the automotive environment. Therefore, in these cases, even in a qualitative way, only rough estimations were available. Nevertheless, a full assessment was infeasible, since anti-tampering solutions and their cost from “proof of concept” to “start of production” phase were not exhaustively investigated and tested, as this was out of DIAS scope. The same goes for the cost estimation of the legislative effort demanded to form and implement regulations amendments or expansions toward anti-tampering.

Conclusively, a robust estimate of the monetary impact of tampering was not feasible via DIAS project research, but follow-up projects could contribute to this effort.

2.5 Potential benefit from anti-tampering legislation

Anti-tampering legislation is expected to both reduce the number of tampered vehicles and mitigate the emissions impacts of tampering by mandating the introduction of more robust emissions control systems. The expected tampering shares and tampering rates resulting from the introduction of anti-tampering legislation cannot be easily estimated. However, the Counterfactual scenario assessed in this study illustrates the maximum theoretical benefits that can be achieved, both in terms of environmental and health impact, in an ideal case where 100% of the tampering would be eliminated.

Measures to address tampering could therefore help avoid up to 12.2 megatonnes of NOx emissions and up to 69.6 kilotonnes of PM emissions between 2022 and 2050, looking at the Worst-Case scenario. With respect to the Central Estimate scenario, emissions savings of 3.7 megatonnes and 41 kilotonnes would be achieved for NOx and PM, respectively. This is equivalent to the emissions produced by up to 53 million non-tampered ICE vehicles in 2030. Additionally, such measures could help avoid between 26,000 and 81,000 premature deaths which equate to between 464,000 and 1,437,000 years of life lost due to poor air quality in the same period.

While overall pollutant emissions and the associated health burden are expected to decrease with time, the share associated with tampering is expected to increase. Without anti-tampering legislation, tampering is expected to still contribute to a significant health burden in 2050. Therefore, even in a case where zero-emission vehicles quickly replace internal combustion engine vehicles, anti-tampering regulation has a key role to play in mitigating the health impacts of road transport.

3 Methodology and structure for the proposed anti-tampering framework

3.1 General guidelines for the regulatory framework

Fundamentally, there are two different principles available to exert legislative control over vehicle emissions: technical requirements and functional requirements. Both options will be explained further:

- **Technical requirements:** This is a prescribed set of clear requirements and/or type approval tests with specific limits that the vehicle should fulfil. The underlying assumption is that if the vehicle which is type approved complies with these technical requirements, the production vehicle will also comply (ex-ante approach). This is a straightforward approach for which the responsibilities are clear: the vehicle manufacturer demonstrates the tests and requirements to the type-approval authority, and there are criteria in place for passing or failing these. That is the main advantage of this approach. Technical requirements are suitable for situations where legislative objectives can be specified as characteristics that the vehicle should embody (e.g. a communication protocol) or measurable values to which the vehicle should comply with (e.g. emission limit values). The drawback is that these requirements are only verified on the one vehicle which is offered at the type approval, so there is no guarantee that all the vehicles on the road perform the same way. For that reason, technical requirements may need to be complemented by Conformity of Production and In-Service Compliance requirements, to demonstrate that once produced or in service all vehicles are in compliance.

- **Functional requirements:** The objective of this requirement is described in qualitative terms of what it should achieve, however the way in which this is realised is left open to the vehicle manufacturer upon approval by the authority. Compliance with a functional requirement is subject to interpretation, which is obviously the main drawback of this option. On the positive side, a functional requirement is not restrictive towards any solution that fulfils the objective, and the chosen approach is based on the performance in practice (ex-post approach). As a result, this approach in principle can facilitate innovative solutions, is technology neutral and may stimulate the most cost-effective solution to achieve the legislative objective. At the same time, regulations on the basis of functional requirements are less prone to becoming outdated as the objective normally remains the same. In contrast, technical requirements need adaptations to cover new technologies or when the existing requirements are no longer adequate.

Before reviewing which specific regulatory options would suit best the requirements following from the DIAS project, let's first put the focus back on the overall objective of the project summarised as follows:
Note that a vehicle can never be made completely tamper-proof since with sufficient budget and effort

> *To prevent or detect any tampering strategies which artificially save fuel consumption, additive consumption or other operational expenses at the cost of higher pollutant emission, during the entire life of the heavy-duty vehicle.*

any system can be hacked. Therefore, in DIAS definition prevention should be such that it renders simply not cost-effective to develop and apply any tampering solution.
If all possible tampering strategies were known or could reasonably be identified beforehand by performing a risk analysis they could be targeted directly through appropriate countermeasures. Such measures could then straightforwardly be implemented as technical requirements. As the manufacturer

knows best how to apply the countermeasures, these requirements are better described in a functional way. For example, the legislation might state that the manufacturer shall develop a monitor to detect the amount of reagent injected, and describes the performance requirements. The manufacturer then has the freedom to develop a reagent monitor using the appropriate technology that achieves the objective in the most effective way. As a result, the legislation remains technology-neutral while does not risk becoming outdated.

However, this might still not be sufficient. For example, if a requirement states that a tampering indicator shall be switched on (e.g., in case component A is detected to be removed or if communication signal B is compromised), the manufacturer is not legally obliged to respond to the removal of component X or compromised signal Y. The tampering industry employs smart and creative ways that look for those weaknesses in the vehicle systems that might be overlooked as a potential risk. As a consequence, each time a new tampering approach has been developed and applied successfully in the market, the legislation would have to be amended to include an appropriate countermeasure.
This cat and mouse game could be prevented if the legislation is extended by a functional requirement to ensure that effective countermeasures are continuously developed and/or updated by the manufacturer to address new vulnerabilities that are being exploited. This will be further detailed in Section 4.3.

3.2 Development of anti-tampering framework

The ultimate goal of the DIAS project is to provide a set of guidelines and recommendations for future anti-tampering regulations. To this aim, an assessment of the existing tampering methods (including devices and services) and their providers was initially conducted [(D2.1, 2020), (D3.1, 2020)]. Then, tampering methods were evaluated by employing a security threat analysis and risk assessment, as well as desk and lab testing, while a set of anti-tampering requirements for the involved end-users was developed [(D2.2, 2020), (D3.2, 2020), (D4.1, 2020)]. As a next step, the necessary countermeasures in terms of tampering detection, protection, and reporting were developed [(D4.2, 2021), (D4.3, 2021), (D5.1, 2021), (D5.2, 2021), (D5.3, 2022)] and evaluated both internally and externally [(D2.3, 2022), (D3.4, 2021), (D3.5, 2022), (D4.4, 2022), (D5.4, 2022)]. Finally, the proposed anti-tampering framework was developed. A relevant workflow incorporating all these steps is presented in Figure 3-1.

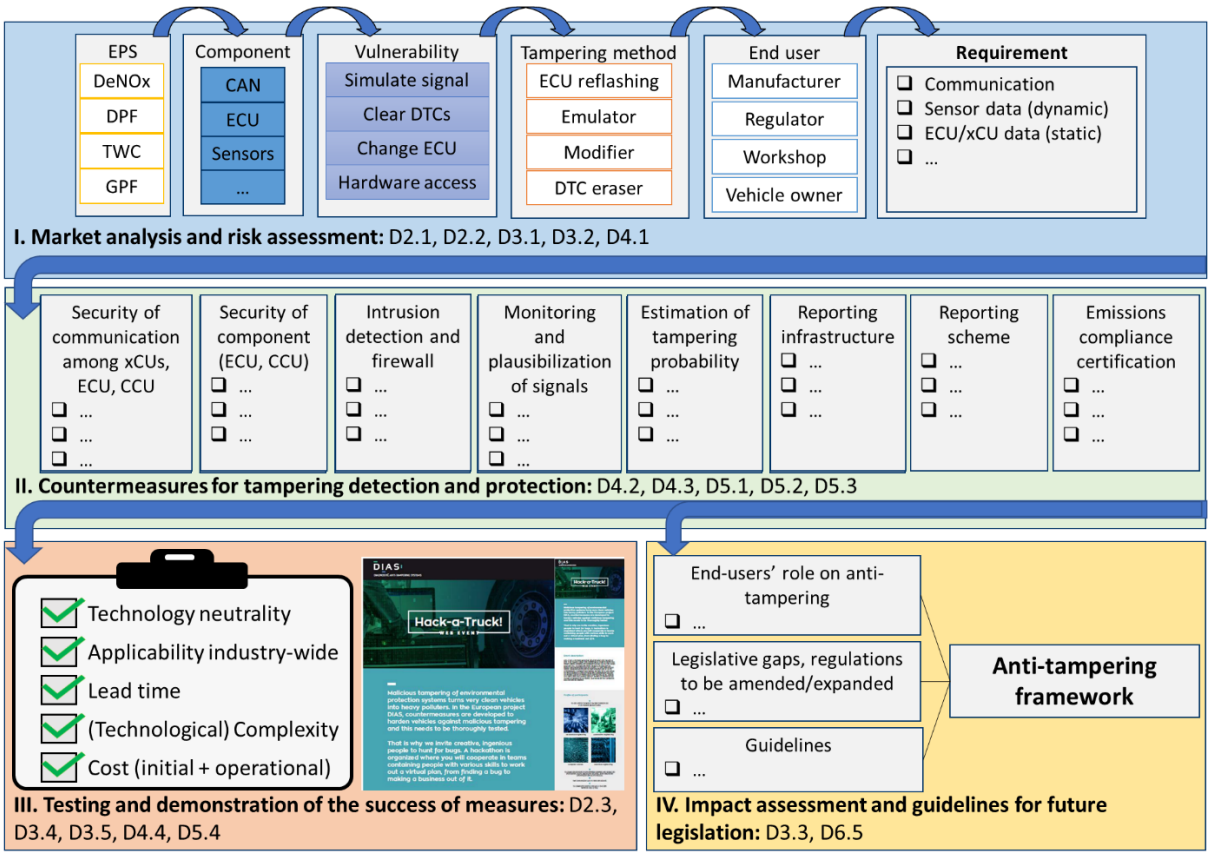


Figure 3-1: Guidelines workflow

Focusing on the anti-tampering guidelines, a 3-step approach was followed:

Step 1: define the end-users who are involved in anti-tampering, specify their roles, and develop the expected guidelines:

- **Original Equipment Manufacturers (OEMs)**
  - Role: Provide vehicle anti-tampering solutions for tampering prevention, detection, and reporting for and after the Type Approval
  - DIAS guidelines: functional requirements
- **Member states**
  - Role: Transpose into national law and enforce tampering-related EU regulatory framework
  - DIAS guidelines: generic guidelines and examples of anti-tampering enforcement measures (e.g. penalties, compulsory controls)
- **Type approval authorities (TAA)**
  - Role and basic DIAS guideline: Ensure that the anti-tampering provisions addressed to OEMs are met by requesting a declaration of conformity, information package and dedicated demonstration tests (proposals for OEMs incorporate the role of TAA). Judge plan and check execution of vulnerability remediation in case new vulnerabilities were found on vehicles in-service.
- **In-Service Conformity (ISC), MaS, (Remote Sensing) authorities**

  - Role: Identify tampered vehicles (based on relative (visual) checks) and report tampering-suspicious vehicles, checking compliance with future regulatory anti-tampering requirements of vehicles in-service.
  - DIAS guidelines: generic guidelines
- **Periodic Technical Inspection centres**
  - Role: Identify high emitters (based on emissions testing) and tampered vehicles (based on relevant (visual) checks), report tampered vehicles, and apply further enforcement actions (e.g. mark as severe omission)
  - DIAS guidelines: generic guidelines and references to best practices
- **Roadside Inspection authorities**
  - Role: Identify high emitters (via remote sensing, plume chasing, or other on-the-road measurement means) and tampered vehicles (based on relative (visual) checks), report tampered vehicles, and apply further enforcement actions (e.g. obligatory PTI check)
  - DIAS guidelines: generic guidelines
- **Workshops**
  - Role: Legitimate use of diagnostic tools and tampering reporting
  - DIAS guidelines: generic guidelines
- **Vehicle owners**
  - Role: Ensure proper and timely maintenance and PTI, and ensure proper "reverting" actions if tampering is concluded
  - DIAS guidelines: generic guidelines

Step 2: review the existing regulations, standards, and protocols concerning emissions, OBD, and in-vehicle (communication and components) security. Based on this review, the gaps, and limitations of current regulations along with the regulations or parts of them to be amended/expanded were identified.

Step 3: provide the OEMs' functional requirements considering all critical aspects e.g. neutrality, applicability industry-wide, implementation time, and overlap of solutions. The DIAS project focused on providing technical solutions for tampering prevention, detection, and reporting. Based on these solutions, the functional requirements to be applied from OEMs were extracted. To retain the technology neutrality of the guidelines, technical details (if needed) are documented only as technical examples. Generic guidelines regarding the other involved parties were also provided.

The specific requirements following the three-step approach will be discussed in detail in Chapter 4.

3.3 Recommended approach for anti-tampering framework for vehicle manufacturers

Combining the guidelines from the regulatory framework and the developed anti-tampering framework, the recommended approach for the implementation of anti-tampering into the regulations is as follows:

- For the type-approval of new vehicles: implement functional requirements for the development of specific countermeasures for vulnerabilities that can be foreseen
- For vehicles in service: implement a functional requirement which prompts the manufacturer to follow up on signs from the market that tampering might be taking place and hence manage threats via a cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating threats i.e. developing upgrades for the countermeasures (vulnerability management)

The specific elements of this framework and the role of the type approval authority are detailed further in Chapter 4. Table 3-1 gives an overview of these elements and the section where they are described.

Table 3-1: Description of chapter 4

Target	Proposed guidelines	Section
Type approval (ex-ante) Section 4.2	I. Risk assessment (TARA)	4.2.1
	II. Dedicated countermeasures	4.2.2
	• Countermeasures derived from TARA and market analysis	4.2.2.1
	• Fundamental countermeasures	4.2.2.2
	○ Secure data exchange	4.2.2.2.1
	○ Secure flashing	4.2.2.2.2
	○ Identification of executed software	4.2.2.2.3
	○ Frequent FCM clear detection	4.2.2.2.4
	○ Estimation of tampering indicator value	4.2.2.2.5
	• Other countermeasures	4.2.2.3
	III. Tampering-related reporting	4.2.3
	IV. Inducement of repair	4.2.4
	V. Demonstrate/declare conformity with legislative requirements	4.2.5
In-service vehicle (ex-post) Section 4.3	Introduction	4.3.1
	Vulnerability management	4.3.2
	Role of third parties	0

The guidelines for the other end-users will be dealt with in Chapter 5.

4 Guidelines/requirements for the OEM

4.1 Current status

Current EU vehicle emissions-related regulations incorporate only a few anti-tampering measures. These measures aim at preventing tampering but there are significant gaps and limitations that tamperers exploit. For example, as documented on DIAS early deliverables (D2.1, 2020), (D2.2, 2020), (D3.1, 2020), (D3.2, 2020), (D4.1, 2020), (D5.1, 2021), existing tampering-related monitors address only a part of tampering attacks. Thus, additional functions should be required.

4.2 Functional requirements for the Type Approval of new vehicles

The functional requirements for the Type Approval of new vehicles are summarised in Figure 4-1:

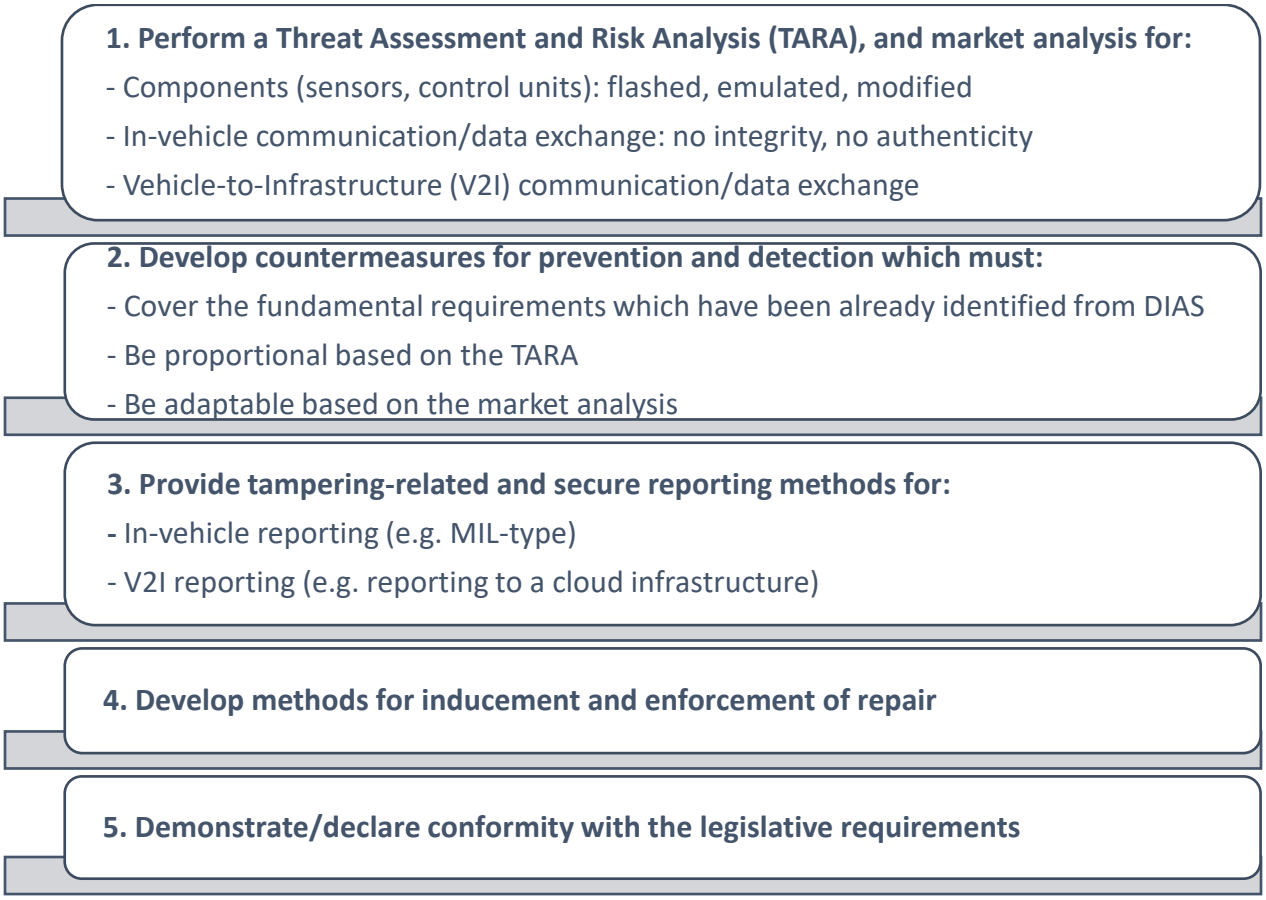


Figure 4-1: Functional requirements (for OEMs) for the Type Approval of new vehicles

4.2.1 Threat Assessment and Risk Analysis (TARA), and market analysis of the tampering systems

OEMs should conduct a Threat Assessment and Risk Analysis (TARA) combined with a market analysis, addressing all known (both hardware- and software-related) attacks.

According to the International Organization for Standardization (ISO) / Society of Automotive Engineers (SAE) 21434, a TARA should contain the following generic modules:

- asset identification
- threat scenario identification
- **impact rating**
- attack path analysis
- **attack feasibility rating**
- **risk value determination**, and
- risk treatment decision

As described in ISO/SAE 21434, organization-specific scales for impact rating, attack feasibility rating and risk value determination can be applied. Focusing on the attack feasibility rating, three approaches are described:

1. Attack potential-based approach
2. CVSS-based approach (Common Vulnerability Scoring System)
3. Attack vector-based approach

When TARA is performed on an EPS, the attack potential-based method (as named in ISO/SAE 21434) should be used. Even though the CVSS method is shown to be one of the most mature methods to perform a TARA, it contains 3 major drawbacks in the context of DIAS:

- CVSS is designed to perform TARA mainly on software components and does not accommodate the attacks shown to be performed in the case of EPS tampering.
- CVSS gives greater attention to attacks that can be performed remotely, which is, again, not relevant in the context of DIAS.
- Finally, CVSS does not take into consideration any environmental or operational impact on the EPS an attack might have.

Also, both the attack vector-based and CVSS-based methods consider that the attacks that require physical access are less feasible, whereas, within DIAS market analysis, it has been shown that most threats to the EPS require physical access. Thus, these methods cannot be used as useful tools to classify the attacks in the context of an EPS, which heavily relies on physical access

However, it should be noted that not even the attack potential-based approach succeeds in fully capturing all the requirements and complexities relative to EPS tampering. For this reason, it is advised that an additional impact category (ISO/SAE 21434, Work Product 15-04) and an additional attack feasibility parameter (ISO/SAE 21434, Work Product 15-06) should be considered. In details:

- An additional impact category should be added called “Environmental impact” that addresses the impact of the attack on the environment and human health.
- The additional feasibility parameter could be called “Financial motive” and should examine the financial gain the professional tamperer and the road user might achieve through the tampering attack (e.g. a road user with a malfunctioning EPS will seek to tamper it instead of performing a costly repair, fleet managers choose to tamper SCR systems to save money on urea costs).

4.2.2 Countermeasures for tampering prevention and detection

4.2.2.1 Countermeasures derived from TARA and market analysis

Based on the TARA and market analysis, tampering attacks are identified, evaluated, and quantified in terms of importance, and in turn, the necessary countermeasures are derived and prioritized. OEMs

should follow this process and develop the necessary countermeasures to appropriately protect the EPSs from tampering in terms of prevention and detection.
Tampering countermeasures can be divided into 2 main categories:

1. Diagnostic functions: These functions aim to detect hardware-related tampering attacks i.e. emulators, modifiers, and DTC erasers:
   - Emulators are devices that inject false sensors' and actuators' signals into the ECU, compromising their data integrity.
   - Modifiers modify sensor signals by hardware means (e.g. using a sensor spacer) to set a false condition of the EPS control logic e.g. to delay the start of reagent dosing via manipulating the exhaust temperature signal.
   - DTC erasers suppress the onboard diagnostics of the vehicle by periodically erasing the fault code storage and sending specific CAN-bus messages.

Even if all the mentioned attacks are (currently) not very robust, there is a relatively great share of the tampering market (mainly regarding HDVs and Non-Road Mobile Machinery (NRMM)) offering these devices.

2. Security functions: These functions aim to prevent tampering attacks that compromise the data integrity of the OEM software (so being undetectable by OBD-related means) to deactivate EPS components partly or totally. These kinds of attacks are called ECU reprogramming or flashing and are widespread in the market offered for LDVs, HDVs, and NRMM. Also, tampering attacks on the data exchange process between Sensor Control Units (SCUs) (of tailpipe exhaust sensors) and ECU should be prevented. Thus, relevant security functions are vital for all types of vehicles.

Tampering-related reporting can also indirectly contribute to tackling tampering. For this reason, it is defined as a separate step of the "anti-tampering" process to be followed by OEMs and it is analyzed in section 4.2.3.

4.2.2.2 Fundamental countermeasures

As documented in DIAS deliverables (D2.1, 2020), (D2.2, 2020), (D3.1, 2020), (D3.2, 2020) and (D4.1, 2020), there are tampering attacks already covering a significant market share, causing a great increase in exhaust emissions and being independent of the EPS technology. Countermeasures targeting these attacks can be characterized as fundamental and should be required regardless of the results of the TARA and market analysis:

- Secure data exchange between SCUs (for direct emission sensing for regulated species) and ECU
- Secure flashing (boot, SW update, transfer of certificates, and tester authentication)
- Identification of executed software
- Frequent Fault Code Memory (FCM) clear detection
- Calculation of tampering indicator value

Note: In future, new tampering attacks can appear in the market that justify the adoption of new fundamental countermeasures. To address this problem without providing continuous regulatory amendments, the EC could assign a relevant expert group to compile and periodically (e.g. every 1 or 2 years) update the list with the fundamental countermeasures (in terms of functional requirements as defined in this report) or compile and update a list of the known tampering methods. The EC already utilizes such methods in its regulations, e.g. in the EU 1939/2019 regulation (European Parliament, Council of the European Union, 2019), an expert group named The Forum for Exchange of Information on

Enforcement is responsible for yearly compiling a list of Auxiliary Emission Strategies which were deemed non-acceptable by Type Approval authorities and this list is made available to the public by the EC.

4.2.2.2.1 Secure data exchange between SCUs (for direct emission sensing for regulated species) and ECU

Modern in-vehicle communications are mainly carried over the CAN bus, where the broadcast pattern gives access to all data exchanges for any entity connected to this bus. As a result, malicious actors (e.g., tampering devices) may (easily) access data exchanges between critical xCUs (e.g. Engine Control Unit, Communication Control Unit, Sensor Control Unit), including the components involved in the EPS. The malicious entities may also alter data, inject new frames, and interfere with the vehicle's normal operation. These tampering attacks – although less robust and frequent compared to ECU flashing - should be characterized as less significant but still critical based on TARA and market analysis documented in (D3.2, 2020) and (D4.1, 2020). This form of tampering is widely advertised on the internet, mainly offered for HDV, and targeting SCR systems. The importance of the secure data exchange between xCUs and ECU can be highlighted in the case of micro-control-based tailpipe exhaust sensors for direct emission sensing of regulated species (e.g. tailpipe NOx and PM). These sensors are indispensable for the effective operation of EPSs (e.g. closed-loop urea dosing control in diesel DeNOx systems), while they are also the basic means of monitoring pollutant emissions for future OBM proposals. A basic aim of OBM is to enable lifetime control of emissions compliance. Tamper-proof tailpipe sensors and sensor-based tailpipe measurements are a prerequisite for all OBM use cases.

Anti-tampering use-case-Generic guideline

To guarantee the **integrity** and **authenticity** of the content exchanged via digital communication protocols such as CAN, data authentication protocols accommodating computationally restricted digital sensors and low-end xCUs should be used. At a minimum, authentication should be applied in the case of micro-control-based tailpipe exhaust sensors for direct emission sensing of regulated species.

Specific provisions should be made for the key distribution among xCUs from different suppliers and in case computationally limited entities such as digital sensors are involved.

4.2.2.2.2 Secure flashing (boot, SW update, transfer of certificates, and tester authentication)

The current implementation of security techniques has proven insufficient to prevent unauthorized flashing of an ECU and keep the data integrity non-compromised. Unauthorized flashing of malicious software to the memory of the ECU should be prevented. At the same time, the possibility to perform authorized flashing should be maintained because this is needed to update the software/firmware of the ECU as part of the normal service of a vehicle with regard to the Repair and Maintenance Information (RMI) regulation (European Commission, 2016). These tampering attacks can be characterized as critical based on (D4.1, 2020) TARA analysis, and they currently cover a great share of the tampering market based on (D3.2, 2020) findings. This form of tampering is widely offered for LDV, HDV, and NRMM, by tuning companies as a service, as a do-it-yourself kit with hardware tools to facilitate the flashing but and is also widely discussed on forums where self-taught experts and hobbyists share information and experiences such as how-to-dos with clear step-by-step instructions and workshop manuals. To address ECU malicious flashing and provide only legitimate one, technical solutions are necessary in terms of secure boot, secure SW update, secure transfer of certificates and tester authentication.

Anti-tampering use-case-Generic guideline

Secure boot

ECU reflashing has been identified as the most important tampering attack. Thus, it is important that ECU is developed with boot security in mind and equipped with Root of Trust (RoT) devices (such as the Trusted Platform Module (TPM)) so that:

- No unauthorized changes can be made to the installed software
- No unauthorized software can be installed or executed and in the case that unauthorized software is detected, execution is blocked

Although other control units (e.g. sensor control unit) may be vulnerable in theory as well, the DIAS evaluations showed that they could not be reflashed for various reasons and thus, requiring a secure boot would not be proportional to the risk.

Secure SW update

To prevent control units from executing unauthorized software or older software that may contain vulnerabilities, it is necessary to implement a secure software update procedure that allows the installation of software only if it is signed by the OEM and only if the software version is newer than the one installed.

Secure transfer of certificates, and tester authentication

End-of-line testers and service centres' tester devices to perform their duties need sometimes unrestricted access to the software and hardware of the ECU. In order to safely perform processes involving testers, a procedure must be in place where the vehicle can safely authenticate the legitimacy of the tester device using a third party such as an OEM or a Certificate Authority.

4.2.2.2.3 Identification of executed software

Anti-tampering use-case-Generic guideline

To verify that a vehicle is equipped with the latest SW and the most up-to-date tampering detection functions, as well as that unauthorized ECU flashing has not been performed, a tamper resilient SW and calibration identifier should be transmitted. This identifier could be either an improved calibration verification number (CVN) or an alternative to CVN. An improved CVN could be built upon the Californian approach to CVN regulations (Bureau of Automotive Repair, Greg Coburn, 2019) but with necessary enhancements. In particular, for being tamper resilient, the identifier's algorithms should allow and accommodate data encryption. In terms of an alternative to the CVN solution, this could be the introduction of a method based on remote attestation techniques. This approach requires the transmission of information to a cloud which currently is not the case for all vehicles. Requirements regarding the transmission of the SW and calibration identifier are analyzed in section 4.2.3 (Vehicle to infrastructure (V2I) reporting).

4.2.2.2.4 Frequent FCM clear detection

Anti-tampering use-case-Generic guideline

FCM clear option has been created to be used by workshops for the confirmation of EPS faults repair. However, since successful tampering comes with the premise that no malfunction indication on the dashboard and inducement-relevant faults are present, tamperers make sure to avoid any fault codes or frequently and periodically delete the fault code memory. Thus, a new function should be introduced to monitor the frequency of the FCM clear and enable the detection of malicious frequent clear of FCM.

Note: Complementarily to this detector, further measures could be applied such as the permanent storage of DTC or else the definition of non-erasable FCM. Nevertheless, this option neither was investigated nor is proposed by the DIAS project due to the already high effectiveness expected by the monitoring of the frequency of FCM clear although the US, China, and Korea have specific requirements for the identification

and storage of permanent DTCs. In detail based on a similar review from International Council on Clean Transportation in 2016 (Posada & German, 2016):

- California Air Resources Board (CARB) and Korea have established clear requirements for storing DTCs in the non-volatile random access memory (NVRAM). This provides CARB and Korea OBD with better protection against clearing DTCs without repairs being made and provides much better technical support for an I/M program based on OBD data.
- The permanent DTCs are required by CARB regulation to remain in memory until the monitor that stored the fault code passes and turns off the Malfunction Indication Lamp (MIL). A permanent DTC in memory without MIL illumination provides the inspector with the information that the vehicle had detected a malfunction before fault information was cleared and the diagnostic that detected the malfunction has not subsequently passed and judged the malfunction to be no longer present.
- An alternative to DTC requirements for China is the adoption of a system that stores the codes outside the vehicle by capturing the OBD information wirelessly and more frequently. The collection system can be located at a roadside station, or via local cellular networks. This type of system is known as Remote I/M, or Continuous I/M.

4.2.2.2.5 Estimation of tampering indicator value

Anti-tampering use-case-Generic guideline

To ensure robust tampering detection (i.e. very low False Positive Rate (FPR) and False Negative Rate (FNR)), it is recommended to estimate the tampering indicator value using a central feature: the tampering detection coordinator. In this way, faults, which can simply occur, would not automatically lead to tampering detection. It can further mask the way the detections work and thus, it will be difficult for tamperers to exploit this functionality and adjust their tampering techniques to avoid a specific detection algorithm.

4.2.2.3 Other countermeasures (examples)

Further anti-tampering security and diagnostic countermeasures should be identified and implemented by OEMs based on their TARA and market analysis to address known and possible future tampering threats. In DIAS deliverables (D4.2, 2021), (D4.3, 2021), (D5.1, 2021), (D5.2, 2021) and (D5.3, 2022) relevant countermeasures are described and in (D2.3, 2022), they are evaluated against specific targets including:

- Technology neutrality and industry-wide applicability: Criterion to evaluate whether the basic principle of the solution can be used in all vehicles and does not require technology-specific know-how, but build upon existing common automotive technology, logical controls, statistical functions, mathematical functions and physical laws. This is based on a theoretical evaluation and it is possible that specific adjustments and modifications are needed for the final implementation in each vehicle/application.
- Lead time: Criterion to evaluate the amount of time that passes from the start of developing a solution until its conclusion. Companies review lead time in manufacturing, supply chain management, and project management during pre-processing, processing, and post-processing stages.
- (Technological) Complexity: Criterion to evaluate the needed technological level for the design and manufacture of a solution, considering its characteristics and performances

- Cost: Criterion to evaluate the estimated financial resources needed for development (including new production lines needed) and operation of the technology used. Accordingly, 2 basic targets are extracted:
    - Development (or initial) cost
    - Operation cost

From DIAS early evaluation (D2.3, 2022) it is shown that there are several "low-hanging fruits" for anti-tampering, meaning that several countermeasures are estimated (some with constraints) as, at the same time, technology-neutral, applicable industry-wide, and of low lead time, complexity, and cost. Relevant examples of these countermeasures along with the threat they address are listed below:

- **Exhaust temperature plausibility monitor (SCR system)** (D5.1, 2021): New ECU-based functions could be added to enable the detection of attacks aiming to reduce the measured exhaust temperature thus, delaying or preventing the activation temperature for dosing Diesel Exhaust Fluid (DEF) to be reached. A potential solution is the use of an advanced temperature model based on heat quantity. The measured temperature signal and the temperature model value at the determined sensor position are monitored and the integrated heat quantity difference between them is calculated. Like when under normal conditions, the measured and the modelled temperature signal are very similar to each other, and the calculated heat quantity difference is expected to be nearly zero depending on model accuracies. In case of mechanical or electrical tampering attacks the temperature level of the measured signal is decreased. Thus, the determined amount of heat quantity difference appears to be significantly higher than normal.
- **Ambient air temperature plausibility monitor** (D5.1, 2021): Complementing current OBD functions, ECU-based monitoring and plausibility checks of Ambient Air Temperature sensor signal could be applied to detect a defective/manipulated ambient temperature sensor that indicates a non-plausible (e.g. high positive constant) value while electrical properties fall in a normal range. Such tampering attacks can completely deactivate DEF dosing. Environmental temperature sensor readings can be modelled regarding the intake air temperature sensor which already exists in the engine architecture. This provides a way of monitoring both sensors i.e. environmental temperature and the intake air temperature sensor
- **NOx sensor diagnoses** (D5.1, 2021): Additional to the current NOx sensor's diagnostics capabilities, new functions could be applied to enable the detection of emulators that send irrational signals concerning fueling and combustion events. To address this attack, a dynamic plausibility monitor for NOx sensors can be used which checks if the NOx signal is falling below a threshold value within a certain time span during the transition to zero fueling (accelerator pedal release). When the engine goes to zero fueling, if the emulator still sends random values, the NOx value doesn't fall below that threshold within the given time interval and a DTC is set. This function, with the necessary adjustments (i.e. thresholds definition), can be applied to other exhaust gas pollutant sensors e.g. NH3 sensors.
- **Lambda sensor diagnoses** (D5.1, 2021): The diagnostics of the lambda sensor downstream of the TWC - or else the heated exhaust gas oxygen sensor (HEGO sensor)-in spark-ignition engines could be enhanced to detect tampering attacks using spacers between the exhaust pipe and HEGO sensor. Relevant enhancements can be built upon the California code of regulations title 13, § 1968.2 (e) (7.2.2) (C) (ii), where monitoring of the slow transition from rich to lean exhaust and the delay of HEGO-response time is required (California state agencies pursuant to the Administrative Procedure Act, 2004). The HEGO sensor's diagnosis function can also include

monitoring a minimum threshold of a rich voltage level ("target rich") and a maximum threshold of a lean voltage level ("target lean") which must be exceeded/undershot during the diagnosis sequence.

- **Adblue refill detection and Observer of Consumption deviation monitor** (D5.1, 2021): Additional to current monitoring functional requirements, new functions could be introduced enabling enhanced (both passive and intrusive) monitoring of DEF consumption to detect emulators that attack multiple components such as pressure lines and dosing valves. Regarding "passive" monitoring, it can be estimated how much DEF needs to be consumed based on the total fuel consumption. Regarding "intrusive" monitoring, a Consumption Deviation Monitor (CDM) observer (based on existing CDM) can be used to trigger a known system behaviour and observe the following results.
- **Emulated dosing control unit (DCU) detector** (D5.1, 2021): Additional to current monitoring functional requirements, new functions could be introduced enabling the detection of an emulated dosing control unit(s) (DCU or DCUs). A relevant detector can be used that monitors the different signals that are relevant for the dosing activity of the DCU. It must be noted, though, that not all features of this functionality may be useful in all applications. For example, the SCR dosing strategy may run on the DCU, where SCR catalyst and NOx sensor diagnosis would practically need to be included there also, such that the detector can only rely on the SCR catalyst temperature.
- **Firewall** (D4.2, 2021): Firewall components could be placed in strategic points inside the vehicle's network architecture to segregate network traffic in a way that malicious traffic cannot spread from one (sub)network to another (thus remaining contained), but also infected payload must not be taken into account. Firewall components shall act in real-time. All detection events created from the Firewall must be logged in a secure environment where unauthorized modification of the logs is not possible. Moreover, the logs must be encrypted and for the establishment of a secure environment, a Root of Trust (such as TPM) shall be used. The IP firewall (module) can leverage the packet filtering capabilities integrated into the Linux kernel via NetFilter and detection events can be recorded in a cryptographically secured logging environment.
- **Intrusion detection system (IDS)** (D4.2, 2021): An IDS could be in place to detect tampered communication messages and communication streams. IDS shall make use of advanced detection rules that inspect packets and streams up to the application level (OSI level 7). Similar to the firewall component, all detection events created from the Intrusion Detection System must be logged in a secure environment where unauthorized modification of the logs is not possible, the logs must be encrypted and, for the establishment of a secure environment, a Root of Trust (such as TPM) shall be used. Finally, detection events shall be recorded in a cryptographically secured logging environment.

Even if the scope of the DIAS project was to identify or develop in-vehicle anti-tampering technical measures for OEMs, the anti-tampering framework concept maintains a broader scope. For example, the United States Environmental Protection Agency (EPA) proposes longer emissions warranty periods which would increase the number of useful life miles covered under the warranty (EPA, 2022). Longer warranty periods may make it less likely for owners to tamper with emissions controls, and more likely that owners will make needed repairs. This countermeasure could be effective but with constraints. At first, the longer warranty period should regard EPSs with higher rates of malfunctions and related costs for repair and therefore increased motivation to be tampered with. Based on DIAS market analysis (D2.1, 2020), (D3.1,

2020), (D3.2, 2020) these EPSs include SCR (Selective Catalytic Reduction), DPF (Diesel Particle Filter), EGR (Exhaust Gas Recirculation) for diesel engines but possibly also TWC (Three-Way Catalyst) for older gasoline engines. Furthermore, the proper increase of the warranty period should be carefully investigated. Motivation for tampering is maintained from the moment the warranty expires, thus, in principle, the longer the warranty period, the greater the effect on anti-tampering. On the other hand, this also results in a greater extra burden on OEMs. Hence, this kind of "non-technical" countermeasures should be investigated in relevant follow-up projects.

4.2.3 Tampering-related and secure reporting

Reporting categorization is often closely related to the relevant "transceivers". For tampering-related reporting two main categories are of interest:

a. In-vehicle reporting
b. Vehicle-to-infrastructure (V2I) reporting

In-vehicle reporting comprises the communication between the vehicle and the vehicle's user(s) which is currently achieved via the Malfunction Indicator Lamp (MIL). MIL is a key component to inform the driver of the emission performance of the vehicle and the need for repair. When activated, it is either flashing or in a steady activated status. The first status indicates a severe fault and serious damage could occur to the catalytic converter or other after-treatment devices if the engine does not stop immediately. The latter is used to indicate problems in a sensor or an aftertreatment device causing increased exhaust emissions, and a visit to an authorized service is mandatory. It is typically in yellow amber, and its shape is a contour of an engine Figure 4-2.

Figure 4-2: Malfunction indicator lamp (MIL)

Every time MIL is activated, a confirmed fault code (Diagnostic Trouble Code, DTC) is stored in the ECU of the car. This code is different for every fault and could be read from a diagnostic device. For the activation of the MIL, an OBD model is used for the diagnosis of every component.

However, currently, activated MIL status does not give any hint for the identification of malicious or non-malicious malfunctions. Based on the tampering indicator value provided by the tampering coordinator (discussed above in 4.2), MIL statuses could be upgraded to incorporate the tampering indicator value either qualitatively (e.g. low, medium, high) or -if possible- quantitatively (e.g. as a percentage). A relevant approach targeting strengthening the MIL has been proposed by the Consortium for ultra-Low Vehicle Emissions (CLOVE, 2021). In this approach, it is suggested to expand current MIL functionalities with additional checks of the state of the vehicle's EPSs and a link to an inducement system. In several OBD 2022 symposium presentations (e.g. (FEV, 2022)), strengthened MIL incorporates the vehicle's EPS state of health based on On-Board Monitoring System emission measurements. However, the OBM system and its components (i.e. sensors mainly) are also subject to tampering. The tampering coordinator may identify such a case since it aggregates all tampering-related ECU-based functions' inputs and it is not exclusively related to tailpipe emissions. Therefore, apart from emissions measurement, the tampering indicator value should be also considered as part of the EPS state of health. Furthermore, the EPS state of

health (and in turn the tampering indicator value) can be linked to the warning and inducement system in a way that the severity of inducement is proportional to the emissions level and tampering probability estimation. An example is analyzed in section 4.2.4.

Nevertheless, tampering indicator and the state of EPS health could be also integrated into a multi-colour MIL. This concept was first introduced by California Air Resources Board in 2019 (CARB, 2019). The MIL can be red, yellow, or green depending on predefined in-vehicle conditions. Although this was a preliminary suggestion not targeting tampering, some tampering-relevant conditions are set resulting in a "red" MIL. These include the use of unauthorized software and whenever a permanent fault code is set.

Vehicle-to-infrastructure (V2I) reporting comprises the wireless exchange of data between the vehicle and surrounding infrastructure, such as traffic lanes, signs, lights, and the cloud. OEMs are already required to continuously monitor and annually transfer fuel consumption data from light-duty vehicles to Member State (MS) or directly to the European Environment Agency based on the latest EU regulations i.e. Commission Regulations (EU) 2019/631 (European Parliament, Council of the European Union, 2019) and 2021/392 (European Parliament, Council of the European Union, 2021c). Relevant latest studies (SERRA, 2020) funded by the EC have developed and proposed standardization requirements for on-off board communication, including robust and safe over-the-air data transfer from the vehicles to the Commission. Upcoming regulations are expected to incorporate such proposals. For HDVs, Regulation (EU) 2018/956 (European Parliament, Council of the European Union, 2018) establishes rules and methods for monitoring and reporting CO2 emissions but no wireless data transfer is needed since CO2 emissions are calculated off-board using vehicle energy consumption calculation tool (VECTO). Moreover, there are no standardized requirements for an Onboard Fuel Consumption Monitoring (OBFCM) device.

Use-cases of V2I reporting

Current EU legislation (regarding both LDVs and HDVs) has no references to V2I tampering-related data reporting. PTI or other periodic checks are generally planned, so many tampering solutions can be "deactivated" only to pass the testing procedure and "reactivated" afterwards. To tackle this problem, reporting "on-demand" of the Member State (MS) in which the vehicle is registered could be available at least in a periodic form e.g. once every 3 months. In this case, a remote reporting system is required including Connectivity and Cloud infrastructures, and relevant procedures. Tampering-related data to be reported may include both emissions and non-emissions data. For continuously measured (i.e. second by second) real-time data, in-vehicle aggregation and pre-processing are necessary to save bandwidth and cloud storage capacity. Regarding emissions-related data (e.g. NOx emissions) aggregation procedures can build upon other regions and projects' procedures such as US/China NOx monitoring regulation and OBM activities (EPA, 2020) (ICCT, 2018). For example, OBM (On-Board Monitoring) as part of EU7 (official announcement is scheduled for November 2022) or OBFCM (On-Board Fuel Consumption Monitoring) infrastructure and rules can be possibly expanded and utilized to also transfer/report tampering-related data. Non-emissions tampering-related data should be more or less already an aggregation result of anti-tampering diagnostics and security functions without needing further aggregation. To identify illegal vehicle ECU flashing and to document that a vehicle is equipped with the latest SW and the most up-to-date tampering detection functions, a tamper-resilient SW and calibration identifier could be transmitted. This identifier could be an upgraded version of the CVN proposed by the Californian Bureau of Automotive Repair (Bureau of Automotive Repair, Greg Coburn, 2019), since current CVN algorithms lack strong cybersecurity capabilities in terms of cryptography. Additionally, it should be verified that the data originate from the ECU and not from a tampering device, and the relevant verification result may be reported. Finally, the anti-tampering diagnostics system via the Tampering Coordinator aggregates all

diagnostics functions' inputs and estimates the tampering indicator value. The latter helps to identify tampering via emulators or modifiers and could be also reported.
A Connectivity infrastructure also allows OEMs to remotely update current tampering diagnostics functions or deploy newly developed diagnostics functions against new tampering threats. These procedures can be also done offline but this is not state-of-the-art. Additionally, a Connectivity infrastructure will enable tampering-related data to be transferred not only from vehicle to MS but also from MS to vehicle. Such a case could be present if a MS introduces a sharable data-driven digital certificate based on PTI (or other authorities) findings. The certificate can be directly related to tampering-related data (emissions and non-emissions data) and relevant reports, and it can be revoked in case tampering is concluded. Furthermore, tampering-related data from the vehicle can be checked on-demand to select suspicious vehicles for roadside inspection or exclude these vehicles from ISC or MaS checks where well-maintained representative vehicles should be selected.

Proposal for V2I reporting

As explained above, there are various use-cases of tampering-related V2I reporting. However, the significance of each use case, the additional burden to OEMs, the lead time needed to provide robust technical solutions, and other important aspects of reporting were not evaluated in the DIAS project. For example, any information reported from the vehicle to an off-vehicle entity can be characterized as confidential data for which the vehicle owner's permission should be granted unless special rules are included in the legislation. Thus, various scenarios, in terms of identifying and handling confidential information to be reported, should be evaluated.

In a conclusion, a reporting system of tampering-related data cannot be proposed as an outcome of DIAS project findings. However:

- If in the context of existing or future regulated V2I reporting activities (e.g. OBFCM), data are requested to be sent remotely, this should be done in a secure way. The anti-tampering security measures regarding this transmission should be extracted based on TARA and market analysis and the DIAS project has developed an exemplary solution for secure data transfer (D4.3, 2021)
- The existing or future regulated V2I reporting activities (e.g. OBFCM or OBM) should examine the possibility of:
    - Transferring/reporting tampering-related data:
        - Tampering indicator value or upgraded MIL status (input from anti-tampering diagnostics i.e. Tampering Coordinator)
        - ECU data verification status (input from anti-tampering security i.e. Communication Security)
        - Secure SW and calibration identifier (upgraded CVN with better cybersecurity capabilities from a cryptographic point of view)
        - Pre-processed and aggregated data of NOx and other exhaust gas pollutants
    - Enabling and implementing remote:
        - update of current tampering diagnostics functions
        - deployment of new developed diagnostics functions against new threats
        - revocation of tampering-related certificate and relevant inducement options set from the MS

Technical example for secure V2I tampering-related data transmission

In DIAS (D4.3, 2021), secure V2I tampering-related data transmission by means of using signed integrity hashes and Self Sovereign Identities has been presented. A hash is a fixed-length value or key that matches, represents, and makes it easier to find or employ, a longer key or string of characters. Tampering-related data are collected in chunks, hashes are computed and then both payload and hashes are transmitted in an independent container on the Connectivity Control Unit (CCU). In detail, the payload is harvested from CAN messages provided every 10ms. Based on a dynamic parameter all the received CAN messages are collected into a so-called chunk (e.g. a chunk of 1.000 messages). Since the defined count of CAN messages to complete a chunk is collected, a hash is generated based on all CAN messages in the chunk, and the hash itself is added to the chunk. This aggregation into chunks is crucial since sending data in 10ms intervals is not feasible for a vehicle and northbound traffic must be saved. Each hash is calculated based on the previously calculated hash to easily identify "altered" data samples. The aggregation process can be seen in Figure 4-3.

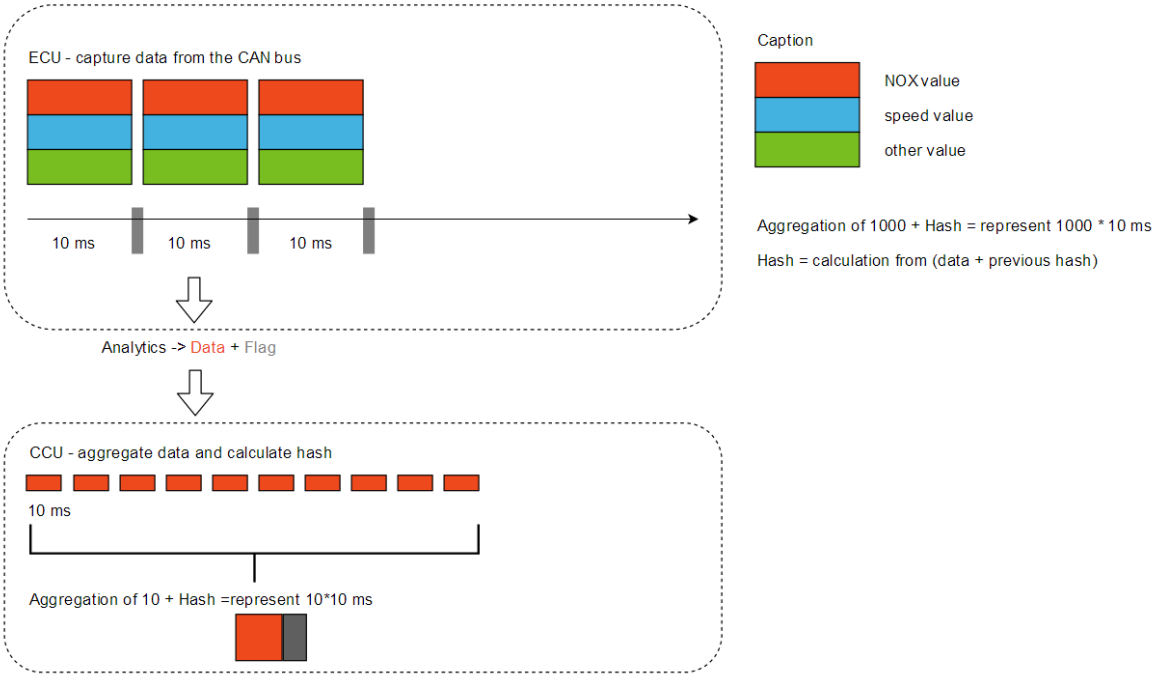


Figure 4-3: Aggregation and hashes (D4.3, 2021)

The data delivery controller employs its in-vehicle Aries agent to sign and submit hashes via DIDComm meaning that each hash sent via the Aries agent is signed with the unique vehicle private key and the resulting message is encrypted. DIDComm is a standard that defines the secure and authenticated communication channel between DID-controlling entities. An example of a Decentralized Identifier (DID)-controlling entity is a Self-Sovereign Identity (SSI) agent. Formally, an agent is a software that enables an entity to assume the role of an issuer, holder, or verifier, and to interact with other agents through peer-to-peer communications. Due to the use of pairwise DIDs, the communication between agents is end-to-end encrypted and is able to provide proof of identity. The most common framework for an SSI agent is the Hyperledger Aries project, in which DIDComm v1 was born. Further technical details are available in DIAS deliverable D4.3 (D4.3, 2021).

4.2.4 Inducement and enforcement of repair

Inducement and enforcement requirements could hinder tampering attempts or oblige the vehicle owner to reverse any tampering attempt. The proposal of in-vehicle reporting of the tampering indicator (section 4.2.3) either incorporated in the current MIL or reported in a separate MIL, (e.g. a new type of multi-colour or multi-stage MIL) is the main feature or the proposed inducement and enforcement requirements.

An example based on best practices is given below.

- For low tampering indicator value, the inducement system will remain disabled and the warning system will indicate the driver to check the malfunction on the next service appointment or the next PTI test. In case the tampering indicator value remains low, a timer or mileage meter can be activated. If the vehicle exceeds the time or distance limit the tampering indicator value will change to medium (thresholds should be defined in a follow-up study).
- For medium tampering indicator value, the inducement system will be enabled and the warning system will indicate the driver to check the system within a predefined time or distance limit. Although the exact thresholds should be defined (possibly in a follow-up study), existing requirements for vehicles that use a reagent for the exhaust after-treatment system could be applicable [Appendix 6 paragraphs 3 and 8 of UNECE R83 (United Nations Economic Commission for Europe (United Nations Economic and Social Council), 2012) and Annex 11 paragraphs 4 and 5 of UNECE R49 (United Nations Economic Commission for Europe (United Nations Economic and Social Council), 2013)].
- For high tampering indicator value, the inducement system will be enabled and the warning system will indicate the driver to act immediately. Stricter requirements based on the current requirements for vehicles that use a reagent for the exhaust after-treatment system could be applicable [Appendix 6 paragraphs 3 and 8 of UNECE R83 (United Nations Economic Commission for Europe (United Nations Economic and Social Council), 2012) and Annex 11 paragraphs 4 and 5 of UNECE R49 (United Nations Economic Commission for Europe (United Nations Economic and Social Council), 2013)].

Different levels may not be useful if the sensitivity of the tampering indicator value is not sufficient. Therefore, it might be needed to use a binary approach (low and high tampering probability).

4.2.5 Declare and demonstrate conformity with the regulatory requirements

The fundamental 'must have' anti-tampering measures shall be implemented by the OEM. To this aim, the OEM shall provide an information package to the TAA and a declaration on fulfilling the requirements. The TAA may ask for dedicated demonstration tests, including reporting of the MIL in the case that tampering is detected by the vehicle. For such demonstration tests, there are no test procedures in place; alternatively, the TAA could demand the OEM to run demonstration tests, tailored to the specific technologies of the emission control system applied.

4.3 Functional requirements for the vehicles in-service

4.3.1 Introduction

The conventional approach for vehicle type approval, i.e. to require the manufacturer to deliver an information package at type approval and where necessary perform demonstration tests, will no longer

be sufficient to safeguard vehicles from future attacks. A reason is that new tampering is developed once there is a demand from the market, for instance when vehicles in-service start to have malfunctions and need repairs and the warranty period is over. Keeping the vehicles that are in-service safe from tampering can only be achieved by bringing in a feedback loop from observations in the market directly back into the type approval process. Effectively, this could be realised by complementing the type approval requirements identified in Section 4.2 with a functional requirement on vulnerability management. This could state that when a new tampering strategy is discovered in the market, the manufacturer can be requested by the type approval authority to assess the risk for its system and - if necessary - to develop countermeasures to close the vulnerability that was exploited. In a certain way, this methodology shows an analogy to the world of aviation safety, where a (near) aeroplane accident is not seen just as an unlucky event but as a sign of an omission in the complex system of safety instructions and procedures which needs to be investigated and repaired. Similarly, a new and successful tampering strategy may be seen as evidence of the vehicle system not being sufficiently robust against tampering. The functional requirement adds the ex-post element that could help to close the loop on unforeseen tampering strategies.

4.3.2 Vulnerability management

By means of monitoring the manufacturer, in collaboration with the TAA but also other National Authorities (such as ISC or MaS), can keep an eye on developments in the market, e.g. by observing information received from the in-service vehicle, in order to find out if there are signs that possibly tampering is taking place or new vulnerabilities are exploited. If the signs are clear, they could then be investigated in detail. Such a statement could be added to the functional requirement, requiring/requesting the manufacturer to deal with any new tampering strategies by vulnerability management.

Vulnerability management is essential for dealing with potential new tampering strategies both for the vehicles in-service and the next generation of vehicles entering the market and is meant to ensure that possible newly found vulnerabilities are resolved. The countermeasures should be selected based on an impact assessment to take into account, for example, the technical constraints which might be different between the vehicle in-service and the next generations of vehicles.

The following (non-exhaustive) list of information sources could be evaluated as input for tampering monitoring:

- Vehicle data communicated to the cloud
- Feedback from vehicle dealers/workshops
- Feedback from periodic technical inspections (PTI)
- Monitoring the offered services and products of tamperers
- Test results from in-service conformity testing or market surveillance tests (ISC and MaS)
- Road-side inspections
- Results from independent third parties

The task to follow-up the above-described activity in collaboration with the concerned manufacturer, could be addressed to the type-approval authority.

4.3.3 Role of third parties

As mentioned above, evidence on vehicles that are tampered with may come from dedicated testing programs initiated by third parties. Contrary to other parties in the legislative context that have a formal

role (e.g. TAA, MaS, MS) they could receive a position in the legislation to allow a route for their observations. Both the position and the route to follow could be laid down. This may look as follows. In the case that tampering activities are observed by third parties or MaS, they can come forward to the type approval authority that could be obliged to evaluate the provided evidence. On the basis of that evaluation, the type approval authority will decide if the evidence is convincing and if so, will start their own investigation while the manufacturer is informed. Based on the outcome of this investigation, the manufacturer may be required to take appropriate countermeasures based on an impact assessment. The countermeasures may need to be different between the next generation of vehicles and the vehicles in service. For example, the ECU capabilities for a vehicle in-service may be not enough to install resource-demanding diagnostic or security solutions. More on the role and responsibilities of MaS can be found in Section 5.4.

5 Guidelines/requirements for other end-users

5.1 Member states' guidelines

5.1.1 Current status

EU member states (MS) are responsible for implementing EU regulations and directives. The tampering-related EU regulatory framework is generally transposed and covered at the national level by national road and motor vehicle regulations. MS are greatly involved in the anti-tampering framework since they are enforcing and regulating the whole framework as the highest authority on the national level. This is succeeded by enforcing prohibitions, roadworthiness inspections (periodic and non-periodic roadside ones), penalties, and regulating reporting from all end-users.

5.1.2 Guidelines (ideas and proposals)

To enforce the anti-tampering framework, steps are needed to ensure and increase the harmonization of anti-tampering measures' effectiveness on every MS but also among all MS.

- **Prohibitions, roadworthiness inspections, and penalties**

  At first, the use, execution, or trade of tampering-related devices/services should be forbidden, and fines should be imposed on anyone involved (e.g. Workshops, Vehicle owners). These prohibitions can be explicitly incorporated into articles relevant to obligations in EU 595/2009 and EU 715/2007 regulations (European Parliament, Council of the European Union, 2009; European Parliament, Council of the European Union, 2007). These obligations should prohibit any EPS or EPS component tampering and should be written -or amended from other EU (implementing) regulations- in such a way that liability can be reliably extracted. Articles relevant to penalties should also make MS responsible to impose effective, proportionate, and deterrent fines for any violation of tampering-related obligations.

  Furthermore, tampering practices should be prevented by legislating relevant checks and reporting implemented by PTI centres and Roadside Inspection (RSI) authorities. More analysis regarding this topic is conducted in sections 5.2 and 5.35.3.

- **Reporting**

  Last but not least, MS should enforce reporting of tampering cases and information. The aim is to create a tampering database which will include the latest tampering indicator value for every vehicle, the result of the previous PTI check and additional information for the discovered tampering attacks in PTI or roadside inspection. In this way, detection of any tampering attack will be reported, and any new attack will be widely known. Appropriate reporting options could be an online web page like in the violation reporting procedure implemented for workshops in California of the US (Acevedo & Yarbrough, 2019). The DIAS proposal is that such a system should be centralized and common for workshops, PTIs and roadside inspection authorities.
  The above concerns many anti-tampering end-users except OEMs. As presented in OEM's section 4.2.34.2.3, V2I reporting will take place only if requested by other existing or future regulated V2I reporting activities (e.g. OBM). OEMs should take care of the secure transfer of tampering-related data which shall be realized only after the mutual authentication of all involved parties, such as the vehicle, the data holder, and the prospective data consumer. MS will play an important role

in this chain by providing/hosting the necessary authorities such as the Vehicle License Authority (VLA) or the Periodic Technical Inspection Authority (PTI) as described in (D4.3, 2021).

5.2 Periodic Technical Inspection centres' guidelines

5.2.1 Current status

Periodic roadworthiness inspection aims at ensuring the vehicle's conformity in terms of safety and environmental performance. PTI legislation describes the parts of the vehicle that should be checked, the visual inspections, the emissions measurement, and the roadworthiness certificate. The emission conformity on PTIs is checked by 2 means:

- Direct measurements of emissions:
  - For diesel vehicles: exhaust gas opacity test, which measures the Particulate Matter (PM) emissions (European Parliament, Council of the European Union, 2014)
  - For petrol vehicles: CO and Hydrocarbons (HC) (European Parliament, Council of the European Union, 2014)
- OBD data: List of DTCs: NOx group for LDVs and class A, B1, B2 for HDVs (European Parliament, Council of the European Union, 2019)

Tampering is a known issue to PTI centres and specific instructions on how to check for tampering evidence are available. Overall, though, the procedures focus only on DPF removal detection while significant reliability issues are also raised.

5.2.2 Guidelines (ideas & proposals)

The proposed guidelines are analyzed below:

- **Advanced emission measurement techniques for all regulated pollutants**: This will allow the PTI centre to discover all high emitters although it is not proof of tampering. As an example, the NOx emissions shall be measured by a testing method which must be chosen, depending on the year of construction of the vehicles and the potentials of the test area, time, cost of equipment, usability and applicability of every MS's competent authority. (CITA, Position Paper: Monitoring of NOx emissions as part of PTI, 2022). Measurement of particle number in the exhaust downstream of combustion ignition vehicles using particle counters approved for PTI measurements at idle conditions, as the New Periodic Technical Inspection (NPTI) working group proposal suggests, should ensure the effectiveness of the particulate filter. A few countries like Germany, Belgium, the Netherlands, and Switzerland already adopted the rules for measuring PN.
- **Advanced visual inspections**: Every inspection centre must carry out visual inspections on the wiring harness of actuators and sensors for modifications and for emulators. Also, the critical EPS components (e.g. DPF, SCR system) should be carefully inspected.
- **Access and evaluation of tampering-related data:** Software and calibration identifiers (section 4.2.2.2.3). must be checked for every vehicle. Also, the tampering indicator value should be checked.
- **Reporting of tampered vehicles**: Member States should host a reporting system for PTIs, workshops and roadside inspections (section 5.1.2). PTIs should provide in this database the result of the latest PTI check, the latest tampering indicator value, and any additional information in case a tampering service or device was identified.

- **Enforcement actions**: Any tampering-related deficiency must be categorized as dangerous deficiency. Also, any dangerous deficiency (either related to tampering or not) should lead to the revocation of the license plate and the owner will have to repair the vehicle and bring the vehicle to the PTI centre within a limited time period (e.g. 10 days).

5.3 Roadside Inspection authorities' guidelines

5.3.1 Current status

The RSI is complementary to the periodic technical inspection and in turn, the purpose of RSI is to ensure road safety and the effectiveness of the exhaust aftertreatment systems by applying unexpected technical inspection. Similarly to PTI, RSI tampering-related procedures including visual inspections and emissions testing are not optimized.

5.3.2 Guidelines (ideas & proposals)

The proposed guidelines focus on advanced emission measurements (to identify all high emitters), advanced inspections for tampering and enforcement actions.

- **Advanced emission measurement techniques for all regulated pollutants:** Currently, plume chasing and remote sensing techniques are used to identify high emitters. New instruments for more accurate measurements and for additional pollutants are necessary. There are already a few projects and activities in this area and therefore, significant improvements are expected in the near future. As an example, NEMO H2020 project is working on a completely new remote sensing technology that will be able to measure emissions (and noise) from individual road vehicles and trains in real-time (NEMO H2020 project, 2022).
- **Advanced inspections**: Every roadside inspector must carry out visual inspections on the wiring harness of actuators and sensors for modifications and for emulators. Also, the critical EPS components (e.g. DPF, SCR system) should be carefully inspected.
- **Access and evaluation of tampering-related data:** Software and calibration identifiers (section 4.2.2.2.3). must be checked for every vehicle. Also, the tampering indicator value should be checked. To make access to these data more efficient, OEMs should collaborate with scan tool manufacturers to provide a harmonized way to access and check vehicle data.
- **Reporting of tampered vehicles**: Member States should host a reporting system for PTIs, workshops and roadside inspections (section 5.1.2). Roadside inspectors should provide in this database the result of their checks, the latest tampering indicator value, and any additional information in case a tampering service or device was identified.
- **Enforcement actions**: Any tampering-related deficiency must be categorized as a dangerous deficiency. Also, any dangerous deficiency (either related to tampering or not) should lead to the revocation of the license plate and the owner will have to repair the vehicle and visit a PTI centre within a limited time period (e.g. 10 days).

5.4 ISC and MaS authorities' Guidelines

5.4.1 Current status

In-service conformity (ISC) and Market Surveillance (MaS) are used to ensure that vehicle emissions comply with pollutant limits throughout the vehicles' normal useful life and under real and normal operating conditions (Real Driving Emissions (RDE) test). ISC regards testing carried out by manufacturers

on in-use vehicles and components, while MaS refers to independent verification testing and inspection carried out by regulatory authorities on in-use vehicles. MaS-related testing can be conducted also by third parties to hold governments and manufacturers accountable. For ISC and MaS testing and inspection procedures, selected vehicles must fulfil certain criteria -regarding proper use and maintenance- to be representative of the whole fleet of each vehicle type. This means tampered vehicles will not be tested unless the anti-tampering system and relevant tampering indicators are cheated.

5.4.2 Guidelines (ideas & proposals)

Even if ISC and MaS procedures do not seem, by principle, to contribute a lot to anti-tampering, there are relevant simple-in-concept measures that would exploit these procedures in terms of anti-tampering. Tampered vehicles found during the vehicle selection process (i.e. inspection) should be reported to the MS database (5.1.2). ISC and MaS inspections should be enhanced in terms of tampering identification methods and effectiveness, similarly to RSI and PTI (described in sections 5.2.2 and 5.3.2, respectively). Finally, the tested vehicles with high emissions that do not have an active MIL during the test and are under investigation from Granting Type Approval Authorities can be also reported to MS for comparison with PTI, or any other relevant source.

5.5 Workshops' guidelines

5.5.1 Current status

Workshops are not active actors in the prevention and reversion of tampering on-road vehicles in regards to the EPS system. The legislation does not provide the necessary motives and enforcement strategies to include workshops in the surveillance scheme of tampering. The Forum for Access to Security-Related Vehicle RMI (SERMI) is the main responsible for workshops' activities surveillance. SERMI scheme defines the procedure for the approval and authorization of independent operators (IOs) to access vehicle security information. However, the current scheme does not grant secure access to EPS-related information.

5.5.2 Guidelines (ideas & proposals)

The guidelines will be divided into two categories:

- Proposals for the necessary changes that should be made on the accessing of information of the EPS as an IO, and the procedure of establishing communication with the vehicles (tester – xCU) in the workshop environment
- Discussion of the necessary actions taken by the workshops in case tampering is detected on a customer's vehicle

The expansion of the SERMI scheme is suggested to protect access to EPS-related information. This can be realized by enforcing accreditation and business activities surveillance on the IOs that wish to gain access to EPS-related information. The SERMI scheme (Figure 5-1) is thoroughly developed and achieves a high level of protection regarding access to vehicle information, thus no changes are proposed in its architecture except the expansion of its role.

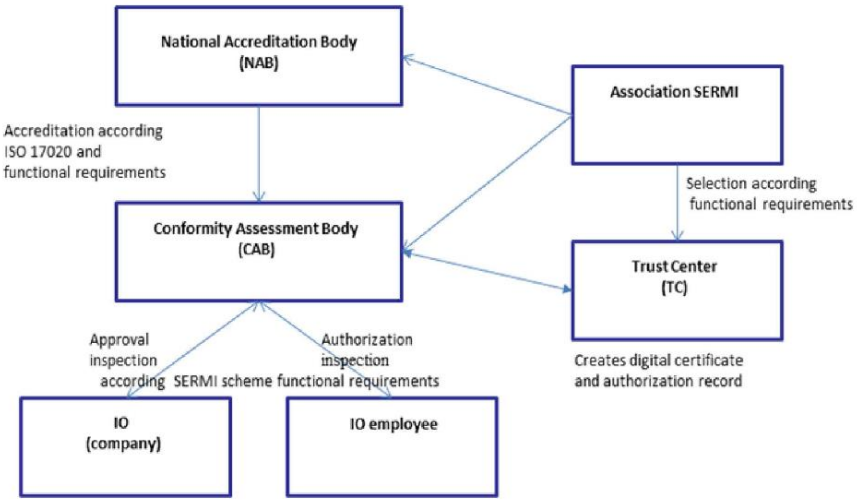


Figure 5-1: SERMI Scheme (European Parliament, Council of the European Union, 2021b)

SERMI scheme is designed to provide a certificate to the IO employee, which mainly enables him to gain access to safety-related information on the OEMs website. Except for the authorized access to information on the vehicle's architecture, it is very crucial to ensure authorized communication between the IOs and the vehicle's xCUs in the workshop environment. Every time an IO's employee is trying to communicate with a vehicle's xCU through a tester device, an authentication procedure should take place to ensure the authorization of the service provider. This way the EPS system will be protected from manipulation in case an unauthorised person tries to override its operation. Both SERMI scheme and the scheme developed in DIAS D4.2 (already shown in Figure 5-1: SERMI Scheme Figure 5-1), make use of X.509 digital certificates in order to verify the identity of the person trying to gain access either to the OEM's website or the vehicle's xCUs. Therefore we propose the use of digital certificates every time someone is trying to communicate with the vehicle's onboard xCUs (X.509 certificates are a convenient solution as already used in SERMI scheme).

The second part concern the necessary actions taken by the workshops in the event of tampering detection and their role in the surveillance of tampering. Ideally, in case tampering is detected during service in a workshop, the environmental protection system should be restored to its proper condition and the customer should be notified. This scenario though raises many difficulties in regard to the required payment of the spare parts and the servicing procedure. Therefore, only notification of the customer about the vehicle's condition and reporting to the relevant national authorities are proposed.

Another topic that needs further investigation is the responsibilities of workshops on the investigation and the reporting of tampering with EPS on vehicles. Reporting to the OEMs any evidence/proof of tampering detected/observed in vehicles brought to them will help in a continuous market analysis. But this can lead to a great workload on workshops, due to constant checking and reporting for tampering, which should be justified by reasonable profit. If tampering is not on the hardware level it is difficult to be detected in the workshop environment, so this should also be taken into consideration. Making tampering detection and reporting mandatory in the workshops, unfair competition may arise in case some IOs systematically circumvent these processes and thus, increasing their profits and customers. Nevertheless, the voluntary submission of tampering-related information on the database hosted by each Member State (5.1.2) is proposed.

5.6 Vehicle owners' guidelines

5.6.1 Current status

In current EU legislation, there is not enough reference to the penalties and the obligations that directly affect vehicle owners with regard to the tampering of the EPS. Some MS have taken provisions on a national level by enforcing post-type approval rules and requirements regarding vehicles' EPS tampering including penalties that concern the vehicle owners.

5.6.2 Guidelines (ideas & proposals)

Vehicle owners should be included in the anti-tampering scheme as active actors. At first, tampering with the EPS, including all its vital components, should automatically impose fines that affect vehicle owners. This way vehicle owners will make sure that the EPS on their vehicle is in proper condition all the time. In EU regulations articles relevant to penalties should also make MS responsible to impose proportionate fines for any violation of EPS tampering-related obligations. In EU HDV type approval regulation (European Parliament, Council of the European Union, 2009) the types of infringements by operators of the vehicles which are subject to a penalty shall be expanded so that they include every part of the EPS susceptible to tampering. These definitions should be incorporated also into EU LDV regulation (European Parliament, Council of the European Union, 2007). Ideally, in case of EPS tampering detection on RSI and PTI, except the penalty/fine that would be automatically imposed on the vehicle owner for circulating with a polluting vehicle, the vehicle owner should be obligated to pay the extra cost in order to revert the EPS system in its original form. Also, in case further inspections are demanded in PTI, from evidence found on RSI, the vehicle owner should pay the extra costs.

6 Conclusions

The introduction and implementation of anti-tampering legislation are expected to significantly contribute to eliminating tampering and its environmental and health impact. 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 shares and rates are:

- 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

The potential benefit is still significant, even if reduced by 10-25%, in case of a faster replacement of internal combustion engine vehicles from ZEVs. Most optimistic estimations for tampering shares and rates result in circa half benefit, while, if the highest available tampering shares and rates are used, the benefit doubles or even triples (e.g. 81,000 premature deaths can be avoided). It is also worth notable that while a decrease with time is expected in overall pollutant emissions and the associated health burden, the share associated with tampering is expected to increase. Therefore, tampering is expected to still contribute to a significant health burden in 2050 and anti-tampering legislation seems to have a key role to mitigate this.

Addressing the ultimate goal of the DIAS project to provide a set of guidelines and recommendations for future anti-tampering legislation, an anti-tampering framework has been developed. Several parties are involved in anti-tampering also called end-users, already from previous DIAS deliverables. A few anti-tampering measures are incorporated in current EU and UNECE vehicle emissions-related legislation (including both regulations and directives), but still, significant gaps and limitations that tamperers exploit are observed regarding tampering-related:

- Monitors and obligations towards OEMs, workshops, and vehicle owners
- Definitions
- Reporting
- Prohibitions and penalties
- Requirements during roadworthiness inspections

The level of involvement in anti-tampering is different for each end-user. In particular:

- OEMs are responsible to provide and keep updated the technical means for tampering prevention, detection, and reporting for and after type approval.
- MS have to transpose into national law and enforce tampering-related EU regulatory framework including relevant obligations, prohibitions, and penalties addressed to all end-users.
- TAA have to ensure that the anti-tampering provisions addressed to OEMs are met by requesting a declaration of conformity and dedicated demonstration tests.
- Roadworthiness inspection authorities (i.e. PTI and RSI) can contribute with high emitters (based on emissions measurement) and tampered vehicles (based on relative (visual) checks) identification, tampered vehicles reporting, and further enforcement actions (e.g. mark as severe omission).

- ISC and MaS authorities, even if targeting proper functioning vehicles, may also identify tampered vehicles by relative (visual) checks and check compliance with future regulatory anti-tampering requirements of vehicles in-service, and then report tampering-suspicious cases.
- Workshops should ensure secure access to EPS-related information and could report the tampering-related information collected.
- Vehicle owners are responsible for proper and timely maintenance of the vehicle EPS, while, if liable for tampering, they should economically undertake the EPS reversion to its original stage in addition to other penalties applied.

DIAS project put a great effort into providing technical solutions from the OEMs' perspective for tampering prevention, detection, and reporting. The concluded OEMs guidelines are summarized as:

- **For the type-approval of new vehicles**: Implement functional requirements for the development of specific countermeasures for vulnerabilities that can be foreseen based on the following steps:
    a. Perform a TARA, and market analysis for sensors and control units that could be flashed, emulated, or modified, and for in-vehicle and V2I data exchange
    b. Develop countermeasures for prevention and detection which must cover the fundamental requirements which have been already identified from DIAS, and be proportional and adaptable based on TARA and market analysis respectively
    c. Provide tampering-related and secure methods for in-vehicle and V2I reporting
    d. Develop methods for inducement and enforcement of repair
    e. Declare and, when requested, demonstrate conformity with legislative requirements
- **For vehicles in service**: Implement a functional requirement that requires the OEM to follow up on signs from the market that tampering might be taking place by managing threats by a cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating threats i.e. developing upgrades for the countermeasures and the inducement of vehicles (vulnerability management). This may include the following elements:
    a. General statement on tampering prevention
    b. Proactive monitoring of vehicle fleet
    c. Allow third parties to supply tampering evidence

Finally, to further support anti-tampering additional anti-tampering measures, classified by end-user, should be also adopted.

7 References

Bureau of Automotive Repair, Greg Coburn. (2019, 10 17). *ON-BOARD DIAGNOSTIC SYSTEM VEHICLE TAMPERING PREVENTION.* Retrieved 11 26, 2021, from ON-BOARD DIAGNOSTIC SYSTEM

CARB. (2018, 11 15). *Real Emissions Assessment Logging ("REAL") will track greenhouse gas and smog-related emissions*. Retrieved 11 08, 2021, from https://ww2.arb.ca.gov/news/carb-gets-real-further-cut-pollution-diesel-and-gas-vehicles

CARB. (2021). "Real Emissions Assessment Logging" (REAL); CCR title 13 1971.1 (h)(5.3) . CARB.

CLOVE. (2021). *Preliminary findings on possible Euro 7 emission limits for passenger cars and LCVs: Additional technical issues for Euro 7 LDV.* European Comission through CIRCAB platform. Retrieved from https://circabc.europa.eu/sd/a/451ffbfb-b095-41bc-a4df-1a15af9f1409/AGVES-2021-04-27-LDV_v7_final.pdf

Dieselnet. (2021). *EU: Periodic Technical Inspections (PTI)*. Retrieved from https://dieselnet.com: https://dieselnet.com/standards/eu/pti.php

EPA. (2020). *Guidance for On-Road Testing Requirements for Enhanced Vehicle Inspection and Maintenance (I/M) Programs.* EPA.

EPA. (2022, March 28). *Proposed Rule and Related Materials for Control of Air Pollution from New Motor Vehicles: Heavy-Duty Engine and Vehicle Standards.* Retrieved from United States Environmental Protection Agency (EPA): https://www.govinfo.gov/content/pkg/FR-2022-03-28/pdf/2022-04934.pdf

European Parliament, Council of the European Union. (2007, June 20). Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6). *Official Journal of the European Union*, 1–16. Retrieved from http://data.europa.eu/eli/reg/2007/715/oj

European Parliament, Council of the European Union. (2009, June 18). Regulation (EC) No 595/2009 of the European Parliament and of the Council of 18 June 2009 on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI). *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/eli/reg/2009/595/oj

European Parliament, Council of the European Union. (2017, June 1). Commission Regulation (EU) 2017/1151 of 1 June 2017 supplementing Regulation (EC) No 715/2007 of the European Parliament and of the Council . *Official Journal of the European Union*, 1–643. Retrieved from https://eur-lex.europa.eu/eli/reg/2017/1151/oj

European Parliament, Council of the European Union. (2018, June 14). Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. *Official Journal of the European Union*, 1–218. Retrieved from https://eur-lex.europa.eu/eli/reg/2018/858/oj

European Parliament, Council of the European Union. (2019, April 23). Commission Implementing Regulation (EU) 2019/621 of 17 April 2019. *Official Journal of the European Union*, 5–28. Retrieved from https://eur-lex.europa.eu/eli/reg_impl/2019/621/oj

(2021a, May 20). COMMISSION DELEGATED REGULATION (EU) 2021/1244 of 20 May 2021. *Official Journal of the European Union*, 1-13. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1244&from=EN

European Parliament, Council of the European Union. (2021c, March 5). Commission Implementing Regulation (EU) 2021/392 of 4 March 2021. *Official Journal of the European Union*, 8–25. Retrieved from https://eur-lex.europa.eu/eli/reg_impl/2021/392/oj

European Parliament, Council of the European Union, 2021b. (2021b, May 20). COMMISSION DELEGATED REGULATION (EU) 2021/1244 of 20 May 2021. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1244&from=EN

GrafanaLabs. (2021). *Grafana*. Retrieved 12 09, 2021, from https://grafana.com

https://www.bosmal.eu. (2021). Retrieved from https://www.bosmal.eu: https://www.bosmal.eu/290-exhaust_gas_opacity_measurements#:~:text=Exhaust%20gas%20opacity%20is%20a,500%20mg%2Fm3.

Ingenieurbüro Lohmeyer GmbH & Co. KG. (2021). *Ermittlung der Emissionen von Kraftfahrzeugen im fließenden Verkehr mit Remote Sensing Detection (Emi-RSD).* Senatsverwaltung für Umwelt, Verkehr und Klimaschutz, Referat Immissionsschutz . Berlin: Senatsverwaltung für Umwelt, Verkehr und Klimaschutz, Referat Immissionsschutz. Retrieved from https://www.berlin.de/sen/uvk/umwelt/luft/luftreinhaltung/projekte-zum-luftreinhalteplan/rsd-abgasmessung/

Pöhler, D., Engel, T., Roth, U., Reber, J., Horbanski, M., Lampel, J., & Platt, U. (2019). NOx RDE measurements with Plume Chasing - Validation, detection of high emitters and manipulated SCR systems. *23rd Transport and Air Pollution* (pp. 556-564). Thessaloniki: Joint Research Centre (JRC), EU. Retrieved from https://publications.jrc.ec.europa.eu/repository/bitstream/JRC117559/proceedings_23_tap_part_ii.pdf

Thürmer, J., & Schuster, M. (2018, April 5). *Illegale Fahrzeug-Manipulationen - Der Abgas-Wahnsinn auf Deutschlands Straßen*. Retrieved from BR Fernsehen: https://www.br.de/br-fernsehen/sendungen/mehrwert/illegale-fahrzeug-manipulationen-abgas-wahnsinn-deutschland-strassen-100.html

Vermeulen, R. J., Verbeek, R. P., & van Goethem, S. (2017). *Mogelijkheden om manipulatie van AdBlue-systemen bij vrachtwagens vast te stellen en terug te dringen - eindrapport.* Den Haag: TNO. Retrieved from http://resolver.tudelft.nl/uuid:42ade085-09da-40e1-bba0-006f0bcad033

Vojtíšek, M., Skácel, J., Beránek, V., & Pechout, M. (2018). Roadside measurement of PM/PN emissions from individual vehicles in Prague. *ETH Nanoparticle Conference.* ETH Nanoparticle Conference. Retrieved from https://www.nanoparticles.ch/archive/2018_Vojtisek_PR.pdf