Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 72 (2023) 2824–2831

Transportation Research Procedia

www.elsevier.com/locate/procedia

Transport Research Arena (TRA) Conference

Tampering of environmental protection systems on vehicles: Status quo and perspectives

Robin Vermeulen[a], Dimitrios Kontses[a], Pavlos Fragkiadoulakis[b], Zissis Samaras[b]

[a]*TNO, Anna van Buerenplein 1, The Hague 2595 DA, The Netherlands*
[b]*Lab. of Applied Thermodynamics, PO Box 458, Thessaloniki, 54124, Greece*

Abstract

Pollutant emissions of road vehicles have significantly reduced thanks to the environmental protection systems (EPS), but tampering with these systems can lead to very low efficiency. In the DIAS project, it was found that there is a substantial market for both light- and heavy-duty vehicles and non-road mobile machinery. The main motives are reduction of costs for repair, consumables and downtime, performance tuning, and increase of the exhaust sound level. Tests with several tampering devices revealed that tampering could deactivate or enable the removal of the EPS, and prevent necessary repair of components without malfunction indication and driver inducement occurring, although several tampering devices and services were not successful. Finally, the testing program enabled the definition of the necessary countermeasures to detect and prevent tampering with these systems.

Keywords: Emissions; Tampering; ECU flashing; Emulator; OBD; OBM; security

Nomenclature

AMOC	Ammonia Oxidation Catalyst	HD(V)	Heavy Duty (Vehicle)
CAN	Controller Area Network	LD(V)	Light Duty (Vehicle)
CCU	Communication Control Units	LNT	Lean NOx Trap
DIAS	Diagnostic Anti-Tampering Systems	MI	Malfunction Indicator
DOC	Diesel Oxidation Catalyst	NH_3	Ammonia
DPF	Diesel Particulate Filter	NRMM	Non-Road Mobile Machinery
DTC	Diagnostic Trouble Code	OBD	On-Board Diagnostics System
ECU	Engine Control Unit	OBM	On-Board emission Monitoring
EGR	Exhaust Gas Recirculation	PM	Particulate Matter
EPS	Environmental Protection System	PTI	Periodic Technical Inspection
EVAP	Evaporative Emission System	SCR	Selective Catalytic Reduction
FCM	Fault Code Memory	TWC	Three-Way Catalyst
GPF	Gasoline Particle Filter	NOx	Nitrogen Oxides (NO, NO_2)

* Corresponding author. Tel.: +30-2310-996047;
E-mail address: zisis@auth.gr

10.1016/j.trpro.2023.11.826

1. Introduction

In the European Union, road transport is a key contributor to air pollution, especially in urban areas (European Environmental Agency, 2020). Due to emissions standards for vehicles, manufacturers have managed to introduce state-of-the-art emission controls and have brought, in most cases, significant reductions in the current emissions levels. However, there is increasingly clear evidence of illegal manipulation of Environmental Protection Systems (EPS). Maintenance and repairs are often necessary to keep the systems in good running order but for some vehicle owners, the associated costs for the maintenance or repairs are a reason to tamper with these systems by disabling them, even removing them completely, or suppressing the systems that are meant to diagnose the systems for malfunctions. Emission control systems with higher rates of malfunctions and related costs for repair or maintenance may therefore pose the largest environmental risk: these are Selective Catalytic Reduction (SCR), Diesel Particulate Filter (DPF), Exhaust Gas Recirculation (EGR) and On-Board Diagnostics System (OBD) for diesel engines, but possibly also Three-Way Catalyst (TWC) for older gasoline engines. These manipulations, known as tampering, lead to substantially increased emission levels of individual vehicles and a substantial increase of the emissions of the EU vehicle fleet (EU, DG Move, 2017) (UNECE, 2018) (EPA, 2020). The tampering is facilitated by an internet market and workshops where plentiful tampering devices and services are offered. However, not much quantitative information is available which indicates the magnitude of the problem i.e., the number of vehicles that are tampered with in the EU.

It is estimated, based on results from road-side inspections of trucks, for instance, that up to 10% of trucks in the EU have been tampered with their EPS. The shares may depend on the location where inspections have been conducted and country of origin of the vehicles. For passenger cars, no such information is available, but there are many cases known where passenger cars or vans were tampered with their EPS. Non-road mobile machinery in the member states of the EU do not require periodical inspection of the machinery to check proper functioning of emissions control systems. Many machines are not registered and thus also not checked for proper working environmental protection systems. Little is known about the tampering shares of NRMM, but clearly also for this category, tampering is offered in workshops and online websites, and tampering is openly discussed on internet fora.

In the framework of the EU H2020 programme “DIAS” (Smart Adaptive Remote Diagnostic Anti-tampering Systems) preventive, diagnostic and reporting anti-tampering countermeasures are developed. Four main objectives were identified to fulfil the final targets of the project:

- Analysis of the tampering market and proposal of the necessary anti-tampering requirements
- Development of countermeasures based on the anti-tampering requirements
- Evaluation of the developed countermeasures
- Development of legislative guidelines and assessment of their impact

The current study focuses on the market analysis of tampering devices, including the assessment of the motives, the categorization of tampering and the analysis of the operation and testing of representative tampering systems. This is done to determine the working principles of the tampering and the vulnerabilities of current emission control systems and serves as a basis for the definition of requirements for the necessary countermeasures to prevent, detect and report tampering.

2. Methodology

The current study is broken down into four main steps:

- Market assessment resulting in an overview of tampering motivations, the tampering market, tampering types
- Determination of a matrix of tampering/vehicle combinations to be tested
- Desk/lab assessment of tampering devices and lab and on-road testing of tampering on vehicles
- Definition of requirements for the development of DIAS countermeasures to prevent, detect and report tampering

The market assessment (DIAS project, 2020) comprised internet market review, interviews with professional tamperers, visits to several tamperer workshops, input from roadside inspections, search in internet forums related to

the tamperers community aiming to determine the market of tampering in terms of size, appearance and involved players, to reveal the motivations for tampering and to identify the different types of tampering offered. Indicatively, 7 professional tamperers with physical workshops were contacted: all of them did not focus exclusively on EPS tampering, but on other applications as well, such as modification of other control units for multimedia/lights and/or performance tuning. Detailed input was provided by 2 of them: one for LD and one for HD vehicles. The tamperers were not informed about the real intention of the investigation on our side, to maximize the quantity and the quality of the retrieved information. Most contacted tamperers have experience on both emulators and ECU flashing techniques and some of them endorse some tampering methods more than others based on their practicability and effectiveness. The tampering practices mentioned by the tamperers were cross-checked either via other tamperers of via the internet. There was a possibility that some of the methods mentioned on the internet, either via internet forums or via other internet sites (e.g., those that sell tampering devices), were outdated or some of those were not as efficient as stated. Therefore, a cross-check of any information is required, to the extent possible, so that tampering practices are assessed in terms of applicability and potential of prevalence in the near future.

The exercise has led to a proposal for a test matrix of vehicle – tampering combinations that pose the largest environmental risk and which should be tested to determine the current vulnerabilities and exploits of vehicles that need to be addressed to harden against tampering by the DIAS concept. An overview of critical tampering techniques was generated.

As a next step, a test programme was conducted to determine the working principles of tampering: 35 different tampering systems were ordered and 32 were received and evaluated in desk tests and on a selection of LDV's (Light-Duty Vehicles), HDV's (Heavy-Duty Vehicles) and NRMM (Non-Road Mobile Machinery) during on-road and laboratory tests applying various tampering types (DIAS project, 2020). For the desk tests, various characteristics of the tampering had been determined and administered: purchase cost, appearance, mounting instructions, claimed functionality. In some cases, devices were dismantled to observe and determine internal components. After desk evaluation, a selection of tampering has been tested on LDVs, HDVs and NRMM during on-road and laboratory tests (Table 2). The market assessment revealed that tampering for the latest generation of vehicles (e.g., Euro VI step D or Euro 6d temp) was hardly available, as the development of new tampering to bypass the latest control features of modern EPS probably takes time. For the second last generation tampering is generously available on the market. Tests were executed without tampering first to verify correct vehicle operation and fault code status. Then the tampering was mounted according to the instructions. In some cases, an ECU had to be handed in to a workshop to conduct the ordered flashing. Vehicles were then tested on the road over defined test trips or in an emission test laboratory on a vehicle test bed. During the tests, CAN bus data streams were recorded and tail pipe emissions were measured. Before and after each test, OBD readings were recorded and malfunction indicator status was noted. Finally, the main directions were defined for the development of the required countermeasures which would harden EPS based on the identified vulnerabilities. These directions are based around three main pillars for the development of countermeasures in the DIAS project, namely: prevention, detection and reporting.

3. Results and discussion

3.1. Market analysis

The market assessment (DIAS project, 2020) revealed that there is a substantial market where tampering is offered for the environmental protection systems of passenger cars, vans, trucks and non-road mobile machinery. The main motivation to manipulate environmental protection systems (EPS) is to avoid costs for repair of malfunctions of the emissions control systems of diesel engines. Environmental Protection Systems with higher rates of malfunctions and related costs for repair therefore pose the largest environmental risk. Other motives mentioned are costs for consumables such as AdBlue and fuel, downtime, performance tuning and exhaust sound level. Performance tuning, the increase of the engine power by re-programming the engine settings, is not considered because the action in itself will not lead to an immediate large increase of emissions if the vehicles still use the original catalysts or filters. Filters and catalysts may however get damaged or degrade sooner when the engine is running outside its original settings. Performance tuning is a known motive to remove catalysts, particle filters and deactivate for instance EGR and in these cases will bring about large increases of tail-pipe emissions.

The systems for which abundant tampering is offered are for LD, HD and NRMM equipped with diesel engines: SCR (Selective Catalytic Reduction), DPF (Diesel Particle Filter), EGR (Exhaust Gas recirculation) and OBD (On-board Diagnostics). Tampering is also offered for gasoline passenger cars. The systems targeted for gasoline cars are the TWC (three-way catalyst) and the GPF (Gasoline Particle Filter). The systems which present a high environmental risk are mainly the environmental protection systems of diesel engines. For the GPF of gasoline fuelled cars there is not yet much information about the durability of the system but opposed to the DPF the GPF, due to its more open and different structure, is expected to be less prone to possible damage of the filter element. Table 1 shows an overview of the environmental protection systems for which tampering is offered, the target and the main motivations to tamper with the respective systems.

Table 1: environmental protection systems, tampering targets and motivations for tampering.

Environmental protection system	Tampering target	Main motivations
DPF (+DOC)	Removal of the filter element	Avoid costs for replacement of filter element
	Avoid replacement of broken filter element	Avoid costs for maintenance, filter cleaning
		Decrease costs for fuel, increase power
		Avoid costs for downtime due to malfunction
SCR (+AMOC)	Stop or reduce reagent dosing	Avoid costs for maintenance and repair/replacement of catalyst and SCR system components (NOx sensor, pump, dosing unit)
	Removal of catalyst	Avoid costs for refills with reagent
	Avoid replacement of broken, worn or aged components (pump, NOx sensor, dosing unit)	Extend refill period
	Suppress AdBlue refill message	Avoid costs for possible downtime
EGR	Valve fixed in closed position or blockage of piping	Avoid costs for repair/replacement
		Performance tuning
		Avoid costs for downtime due to malfunction
TWC	Removal of catalyst	Avoid costs for repair/replacement of catalyst and system components (lambda sensor)
	Avoid replacement of broken or worn/aged components (catalyst, lambda sensor)	Probably a niche mostly for performance tuning
OBD	Deletion of trouble codes, MI off, prevent inducement	Supress DTCs, Malfunction indicator and inducement
		Bypass periodic inspection with removed, deactivated or faulty parts (e.g., DPF, EGR)
		Avoid costs for repair/replacement
		Enable tampering of other systems by deleting the trouble codes arising from the tampering of these systems
		This may affect all environmental protection systems
GPF	Removal of the filter element	Increase engine power output
		Change exhaust sound
		No indication that cost of replacement is a motivation, but there is no long-standing experience or information about GPF durability.
New environmental protection systems for which so far, no tampering is reported		
LNT	Possible future problem: Removal of the catalytic element	No tampering device or service found.
Other types of environmental protection systems possibly affected		
EVAP Canister	Removal of canister	Avoid costs for repair/replacement
Start-stop	Prevent engine turning off	Fast engine response from stop
		No hindrance by start-stop interventions

The majority of the tampering devices and tampering services are installed and programmed by experienced mechanic specialists (aided by programmer specialists in case it concerns ECU tampering) in tuning workshops, but simple emulators can also be installed by less experienced individuals and vehicle owners. In public and non-public

internet fora information about installation instructions, tools and fixes to facilitate owners or specialists to tamper, is discussed and exchanged.

A list was generated with tampering devices and services found online in the EU. Four main tampering types and various sub types were identified by the market assessment and were selected for testing to determine and verify working principles and to reveal the vulnerabilities of the vehicle on-board systems.

ECU flashing: The main category which poses the largest risk is ECU flashing. ECU flashing is offered for LDV, HDV and NRMM. Dedicated flashing tools are offered for professional use in workshops or for use by the owners. The tools support flashing very large amounts of ECU types, from older ones to most recent ones with newly supported applications coming out frequently. The main methods for ECU flashing are:

- Dedicated flashing tools connecting to OBD port or engine control unit.
- Third-party service tools connecting to OBD port.
- Opening engine control unit connecting to the internal circuitry to microprocessors
- Older types: Replacing chips in the engine control unit or removing chip and flash on external bench.

For the latest generations of ECUs mainly the OBD port is used to flash malware to the memory of the ECU. The malware may serve either one or various purposes depending on the tampering motivation. For instance, disable EGR, AdBlue dosing, removal of filters/catalysts, suppress DTCs, MI and inducement, increase the torque/power output of the engine.

Emulators: Emulators are small micro-controllers which achieve the tampering goal by emulating and injecting various false signals to bring control systems in an inactive state or within margins of seemingly correct state of operation. A distinction is made between emulators that are meant to deactivate or reduce AdBlue dosing, leave a broken NOx sensor on a vehicle or enable removal of a SCR and/or DPF or GPF. Emulators functionality may entail automatic DTC erasing. Emulators are mostly sold for trucks and NRMM (both agricultural tractors and construction machinery). Emulators seen on the market target mainly the SCR system, to deactivate or reduce the AdBlue dosing or to hide a broken NOx sensor for detection by OBD. In the case a vehicle uses a separate module to control the aftertreatment, emulators require de-activation of the whole module which means that not only the SCR functionality is stopped, but also the DPF needs to be removed because the module can't command active regenerations anymore. Emulators for DPF or GPF removal at present are not frequently offered for LDV and HDV. DPF emulators seem to be offered more for NRMM, possibly because the usage profiles with low loads may cause clogging of the filter. In these cases, for the same reasons, problems with the SCR system may also arise providing a motive tampering the SCR. For NRMM, also combined SCR+DPF emulators are offered that would allow removal of SCR as well as DPF from the machinery. For GPF removal on gasoline cars, the offerings found on the internet aim to increase performance and/ or sound level of the sportier vehicle types.

Modifiers: Modifiers concern a simpler form of signal manipulation compared to emulators and offset a signal value to bring control systems in an inactive state or within margins of seemingly correct state of operation. These are mainly temperature sensor resistors, potentiometers and bushings for SCR, lambda sensor mini-catalysts and spacers for TWC, and pressure sensor modifiers for DPF/GPF.

OBD eraser: This functionality, offered in various forms, can temporarily delete diagnostic trouble codes or is used in an emulator to frequently delete error codes caused by the components that are removed, deactivated or faulty. These can be dedicated OBD DTC eraser, part of service tester or OBD scanner tool or part of emulator.

The cost for tampering ranges from a few Euro's to about 1000 Euro for individual vehicles but depend on the tampering goal. ECU flashing can be done in a workshop (150 Euro for a single job, e.g., EGR, SCR, or DPF up to 900 Euro for a truck for multiple jobs (EGR+SCR+DPF). An ECU reflash can also be done by a non-professional by means of a dedicated tool (100-1500 Euro). The tool can be purchased to flash the ECU images that can be purchased separately (about 300 Euro per flash) or together with the tool. Tool providers also sell subscriptions for the use of more ECU images. One workshop mentioned 30 kEuro for a single year subscription to use all images the tool provider offers. More extended tools can handle more electronic functions e.g., immobilisers, chassis, engine, etc. are more expensive. Emulators can be as cheap as 25 Euro but are typically sold for around 300-500 Euro. Emulators with combined functions to delete SCR and DPF as offered for instance for NRMM engines are sold up to about 1000 Euro. The modifiers are simple tampering devices which may cost a few Euro's to about 35 Euro. Costs for the devices exclude costs for installation.

3.2. On-vehicle assessment

A selection of the purchased tampering was applied in vehicles. The main goal was to understand the working principles of the main tampering types and to determine the vulnerabilities of the current environmental protection systems. Another goal was to check the claims that were made by the tampering provider about the functionality of the device or service. A share of the tampering worked right from the start after installation, meaning that the target system could be deactivated or removed and no diagnostic trouble codes, malfunction indication or driver inducement occurred. The tampering tested was not all without flaws, meaning functionality claims were not always met. In several cases, the tampering did not work at all, leading to DTCs or in the case of one ECU flash lead to DTCs that could be resolved by a fix. An ECU flash that concerned the EGR, SCR, DPF-delete was tested on one truck led to diagnostic trouble codes related to the EGR, but SCR and DPF were deactivated and could be dismounted respectively without DTCs. The SCR and DPF flash tested on the passenger car worked, but DTCs related to the EGR showed up. After receiving a fix from the supplier no DTCs showed up. One emulator for an NRMM wasn't working, meaning that it did not result in the claimed effect, to stop AdBlue dosing. Another emulator for a HD truck broke during installation. Two emulators for a HD truck caused DTCs to show up. Two DTC erasers tested on a NRMM didn't work. A DPF emulator for a passenger car did not work even after modifications offered by the provider. Two of the three TWC modifiers lead to DTCs.

Table 2: overview of the tampering and the impact of the tampering on the targeted systems and OBD of tampering that was tested on vehicles, either on the road or in a test lab on a chassis dynamometer.

	ECU flashing	**Emulators**	**Modifier**	**OBD DTC eraser**
HD1 diesel ***(N3, prototype VI-D)***	SCR: no dosing, DPF, EGR delete → No AdBlue dosing, EGR delete caused DTC	SCR-AdBlue → No AdBlue dosing, no DTC	EGT resistor @130°C → No AdBlue dosing, no DTC after short test, EGT bushing → AdBlue dosing shortly delayed, no DTC, AAT @-21°C → No AdBlue dosing, no EGR, no DTC	
HD2 diesel ***(N3, VI-C)***		SCR-AdBlue → No AdBlue dosing, 1 case with 3 DTCs, 2 cases without DTC, NOx sensor →, No AdBlue dosing, 1 DTC		
HD3 diesel ***(N2, VI-D)***		SCR-AdBlue → AdBlue dosing reduced by 50%		
LD1 diesel ***(M1, EU6c)***	OBD EGR/SCR/DPF → Worked, some DTCs after 1st EGR test (a fix solved this), Flashing pins EGR/SCR/DPF → Worked without DTCs	DPF emulator → Not working		
LD2 diesel ***(M1, EU5)***			Lambda sensor spacers → 1 case with DTC, 1 without DTC, TWC mini catalysts → 1 case with DTC, 1 without DTC	
LD3 diesel ***(M1, -)***			Bushings EGT → AdBlue dosing slightly delayed	
NRMM1 diesel ***(Stage IV)***		SCR AdBlue → Not working, NOx sensor → Not working		DTC eraser → Not working (2 cases)
NRMM2 diesel ***(Stage IV)***		SCR AdBlue → AdBlue dosing stopped, no DTC		

Depending on the components affected, the currently available tampering of the SCR and/or EGR system generally results in a large increase of the NOx tail-pipe emission and when a DPF is removed, in a large increase of the particulate emissions.

3.3. Anti-tampering requirements

The market assessment and the testing program revealed the working principles of four main categories of tampering and the vulnerabilities of current environmental protection systems. This procedure enabled a preliminary definition of requirements to detect and prevent these known tampering techniques. Nevertheless, this is not an exhaustive list and also, a future-proof tampering approach should additionally consider reporting solutions (e.g., to a cloud) and diagnostic solutions (e.g., anomaly detection techniques) for future unknown tampering. These are developed in the last phase of DIAS project and will be compiled in a set of draft legislative requirements. The preliminary requirements can be viewed from the perspective of manufacturers, workshops, Periodic Technical Inspection (PTI) authorities, roadside inspectors and vehicle owners.

3.3.1. Manufacturer requirements

Manufacturer requirements are categorized based on the application field:

ECUs/xCUs: ECUs are units with advanced processing capabilities, which are therefore capable of providing diagnostic and security features. ECUs should support security features (e.g., secure boot capability, secure software update capabilities, code signing, authentication, data integrity in case of CAN transmission and generation of secure keys. The term xCU refers mainly to sensor or communication control units which currently have limited (compared to ECUs) processing capabilities and thus, only part of the aforementioned anti-tampering features can be applied. Communication Control Units (CCUs) should also meet some additional requirements due to the communication nature: the communication with the backend should be protected in terms of integrity, access should be controlled for read/write purposes, private keys and certificates should be stored in a secure manner, and software updates for secure software should be supported.

Sensor data (Digital sensors): Digital sensors include the cases of NOx, PM, Lambda, Delta-P, NH3 and PM sensors. These sensors do not transmit raw signals. They communicate with the xCUs via digital messages. All affected EPS-related digital signals should be checked using monitoring dynamic, offset or plausibility functions. As an additional requirement, Diagnostic Trouble Code (DTC) errors, which are related to the EPS sensors should be checked in terms of the clear events frequency: threshold values of the frequency of FCM clear events should not be exceeded.

Sensor data (Analog sensors): Analog sensors include temperature, pressure, Urea tank level and position sensors. All analogue signals should follow expected patterns. For example, the tank level and EGR position cannot be constant all the time. Also, they should be checked against other related/correlated signals and tested against plausibility checks.

Communication (CAN): CAN is the main protocol of communication in automotive systems between xCUs and Digital sensors and therefore poses a critical vulnerability in terms of tampering targets. The CAN communication of vulnerable components should be protected through authentication and for messages integrity, support secure key generation, secure key storage and secure key exchange in end nodes.

3.3.2. Non-manufacturer requirements

Requirements for workshops, Periodic Technical Inspection (PTI) authorities, roadside inspectors and vehicle owners are mostly of generic nature regarding the type of EPS. Their role is defined in two main directions: to perform the appropriate checks to find tampering and to report tampering to the appropriate authorities (not relevant for owners).

4. Conclusions

The market assessment of cheating devices and the testing programme provided valuable details and directions for the main tampering types, their operation principle, the vulnerabilities of the environmental protection systems and the requirements for anti-tampering solutions. There is a market for tampering with environmental protection systems because a share of vehicle owners declares economic benefits above obligations to properly maintain their vehicles. Tampering is mainly done to prevent costs for repair, maintenance or consumables necessary for a durable, effective application of environmental protection systems over the lifetime of a vehicle. Environmental protection systems, necessary to control the pollutant emission of diesel as used in passenger cars, vans, trucks and non-road mobile

machinery, are mostly targeted. Tests demonstrated that tampering can successfully deactivate environmental protection systems, enable the removal (of parts) of environmental protection systems or prevent necessary repair of components which are essential for the correct operation of environmental protection systems, without malfunction indication, diagnostic trouble codes and driver inducement occurring. The quality of the tested tampering is mixed. Several devices did work without any diagnostic trouble codes, malfunction indication or driver inducement, but also some devices (Engine control unit flash, emulator, three-way catalyst bushing, temperature sensor modifier) lead to trouble codes or hardly work (temperature sensor bushings). For some tampering (engine control unit flash) the provider fixed initial problems after which the tampering worked as claimed. Some other devices did not work at all (emulator, three-way catalyst bushings). Different working principles of tampering have been identified and tampering has been categorized. Engine control unit flashing is seen as the prevailing method used in modern vehicles and machinery, potentially affecting several environmental protections systems. Emulators, however, are still widely offered for trucks and non-road mobile machinery, also for the newest generations.

Based on the observed tampering techniques and vulnerabilities exploited, preliminary requirements are defined which shall be used as guidelines for the development of new functions for the detection or prevention of tampering and which would ensure that the OBD will detect faulty components of the environmental protection system. The end-user requirements are formulated based on the outcome of the verification of tampering practices. Most of them target manufacturers and are proposed measures to prevent unauthorized exploitation of all the EPS related components. These include sensors, control units and CAN protocol requirements.

In the DIAS project, ‘level 1’ countermeasures were developed to prevent or detect current known tampering methods. In a follow-up stage, advanced detection method for future unknown tampering and a cloud-based reporting solution that reports tampering in a cloud environment (DIAS ‘level 2’) were developed. The outcome of the DIAS project will be a valuable input to developments for the Euro7 emission legislation, which aims at securing low emissions over the lifetime of a vehicle via On-Board emission Monitoring (OBM). OBM will continuously check the emissions level during the operation of a vehicle and will have to rely on emission data and parameters from the vehicle. It is therefore essential that this data is secured and cannot be tampered with. DIAS ‘level 1’ and ‘level 2’ countermeasures can provide the necessary tools to prevent, detect and report tampering with environmental protection systems of future vehicles.

Acknowledgements

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

References

DIAS project. (2020, March 31). D3.1. Retrieved from DIAS: https://dias-project.com/sites/default/files/Deliverables/D3.1-Cheating%20devices%20and%20testing%20matrix_0.pdf

DIAS project. (2020, December 23). D3.2. Retrieved from DIAS: https://dias-project.com/sites/default/files/Deliverables/D3.2%20-%20Status%20quo%20of%20critical%20tampering%20techniques%20and%20proposal%20of%20required%20new%20OBD%20monitoring%20functions.pdf

EPA. (2020). Tampered Diesel Pickup Trucks: A Review of Aggregated Evidence from EPA Civil Enforcement Investigations. Retrieved from https://www.epa.gov/sites/production/files/2021-01/documents/epaaedletterreportontampereddieselpickups.pdf

EU, DG Move. (2017). Discussion on tampering with the exhaust emission control system, point 4 of the Summary Report of the Roadworthiness.

European Environmental Agency. (2020). Air quality in Europe. report: EEA. Retrieved from https://www.eea.europa.eu/publications/air-quality-in-europe-2020-report

UNECE. (2018). Tampering of Air Emission Control Systems. Retrieved from https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/WP29-175-07e.pdf