Rethinking transport
27–30 April 2020

TRA 2020 HELSINKI

Proceedings of 8th Transport Research Arena TRA 2020, April 27-30, 2020, Helsinki, Finland

Next generation of vehicle diagnostics based on advanced on-board monitoring and cloud-based diagnostics

Savas Geivanidis[ab], Zissis Samaras[a]*, Markus Willimowski[c], Ian Faye[c], Obaid Ur-Rehman[d], Christof Schernus[d], Robin Vermeulen[e]

[a]*Lab. of Applied Thermodynamics, PO Box 458, Thessaloniki, 54124, Greece*
[b]*International Hellenic University, 14th km Thessaloniki - Moudania, Thermi (Thessaloniki) 57001 , Greece*
[c]*Robert Bosch GmbH, Postfach 30 02 40, Stuttgart 70442, Germany*
[d]*FEV Europe GmbH, Neuenhofstr. 181, Aachen 52078, Germany*
[e]*TNO, Anna van Buerenplein 1, The Hague 2595 DA, The Netherlands*

Abstract

This paper presents the architecture and elements of an advanced diagnostic and emission monitoring system to eliminate the risk of interventions to the vehicle that would lead to emission increase. The designed system will be implemented on a demonstrator vehicle within the framework of the Horizon 2020 project with acronym DIAS funded the European Commission. Firstly, all possible improvements to the existing on-board detection logic (Level 1 measures) are implemented, to demonstrate on one hand demonstrate the feasibility of having more robust conventional systems in a framework for intermediate regulatory steps. On the other hand, it will demonstrate that there will still be weaknesses not possible to be addressed by this conventional approach. This system will include advanced models, virtual and hardware sensors etc. The advanced diagnostic system (Level 2 measures) to enable very robust monitoring will be built using advanced remote cloud-based architectures for data collection and processing.

Keywords: tampering; emission reduction systems; on-boarding diagnostics; on-board monitoring; cloud-based diagnostics; anomaly detection

* Corresponding author. Tel.: +30-2310-996202;
E-mail address: zisis@auth.gr

Nomenclature

ADAS	Advanced driver-assistance systems
CAN	Controller Area Network
CB	Communications Board
CCU	Connectivity Control Unit
DEF	Diesel Exhaust Fluid
DIAS	Smart Adaptive Remote Diagnostic Antitampering Systems
DPF	Diesel Particulate Filter
DTC	Diagnostic Trouble Code
EC	European Commission
ECU	Engine Control Unit
EGR	Exhaust Gas Recirculation
EPS	Environmental Protection Systems
EU	European Union
FCM	Fault Code Memory
GA	General Assembly
GPF	Gasoline Particulate Filter
GPS	Global Positioning System
HDV	Heavy-Duty Vehicles
I/M	Inspection and Maintenance
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
MIL	Malfunction Indicator Light
OBD	On-Board Diagnostics
OBM	On-Board Monitoring
ODS	Overall Diagnostic System
OEM	Original Equipment Manufacturer
PCs	Personal Computer
PEMS	Portable Emissions Measurement System
PM	Particulate Mass
PN	Particulate Number
SCR	Selective Catalytic Reduction
SDG	Sustainable Development Goals
SEMS	Smart Emissions Measurement System
TA	Type Approval
TRL	Technology Readiness Levels
TWC	Three-Way Catalyst
VIN	Vehicle Identification Number
WP	Work Package
xCU	various Control Units

1. Introduction

The primary target of DIAS is to harden vehicle environmental protection systems (EPS) against tampering. This means that any changes in hardware, software that degrade the performance of the EPS will be prevented or detected. In case of a detection the information about tampering is available and is used to introduce countermeasures like e.g. the activation of the driver inducement system. In general, it is nearly always the vehicle's user or operator tampering the EPS for economic advantages; either to reduce fuel or urea costs, or to avoid costly repairs of aged or malfunctioning equipment. It is now clear that supplying tampering devices or approaches has become a huge business that appears to have widespread usage that traditional OBD cannot prevent since they were designed and developed to inform users about malfunctions of systems and components and to enable the workshop to repair. DIAS takes a two-step approach to that. The first step involves implementing measures that take early action against these activities, and a second step prepares methodologies for dealing with

tampering attempts in the future that are currently unknown. Thus, it takes into account that in case of upcoming new tampering effective countermeasures can also be applied on vehicles being already in the field to prevent the environment from pollution.
These systems are intended to operate throughout Europe and even on a global scale and will take advantage from future connectivity that also represents, at the same time, a challenge for the systems.

DIAS involves the major players and stakeholders from the main scientific, technical and logistical domains. The partnership includes the main experts who contributed to the latest on-board diagnostics (OBD) related regulations in the EU, research providers with extensive OBD and emissions expertise, a major automotive supplier with expertise in the Internet of Things (IoT), data security experts, a global heavy-duty OEM and several institutions from the public domain that can substantially contribute to the thorough testing, analysis and acceptability of the solutions to be proposed.

1.1. Background

Emissions standards for vehicles have managed to introduce state-of-the art emissions controls and have brought, in most cases, significant reductions in the actual emissions levels. However, there is increasing clear evidence of illegal manipulation of emission control systems by vehicle owners (European Commission DG Move, 2017; Pöhler, 2017; United Nations Economic Commission for Europe, 2018). These manipulations, known as tampering, substantially affect the emissions of the tampered vehicles, by bringing them back to uncontrolled conditions and hence may constitute a significant threat to the efforts to improve air quality. The reasons for tampering are mainly cost related: avoidance of the costs for consumables (reagent AdBlue), improvement of fuel economy and avoidance of necessary maintenance or repair. Current tampering can be the deactivation of the SCR dosing system, the removal of the DPF or the deactivation of EGR system. Methods that can be applied by the cheaters to remain undetected are either mechanical (e.g. physical modifications to sensors), software (e.g., modification of ECU variables (ECU flash) etc.) or electronic hardware (e.g. manipulation of values in the CAN message or of physical sensors by using emulators). An exhaust emissions control system may be tampered with for several reasons ranging from economics to increasing power or, or in rare cases, malicious behaviour. These systems are being offered openly in the internet and by ‘tuning’ workshops. Alone for Selective Catalytic Reduction (SCR) manipulation, there at least 100 companies worldwide (mainly in Europe but also from China) offering kits for purchase with prices ranging from 10 to 500 €.

In early 2017, it was discovered that the SCR systems of up to 20 per cent of eastern European heavy-duty vehicles on German roads are suspect of being manipulated. Reports by Swiss authorities indicate that in Switzerland vehicles have been caught, with basically in hardware manipulations (mostly SCR emulators and simple built-in potentiometers that stop the dosing of the reagent which is needed for the operation of an SCR system to reduce diesel engine NOx emissions) (Switzerland, 2017). UK reports that 8% of heavy-duty vehicle were found to have a cheat device. However, tampering may well not be detected in every case. In particular, the initial suspicious of tampering is difficult to detect without an extensive review of the vehicle. Additionally, it has been reported that the Swiss border police have very effective at massively reducing tampering by checking vehicles at the border from fleets that have already been caught.

Moreover, removal of the Diesel Particulate Filter (DPF) leading to elevated particulate number (PN) and particulate mass (PM) in the exhaust gas, is also linked to passenger cars. Even though the DPF has a life expectancy of 150 – 200.000 km in cars, DPFs tend to "fill up" much more quickly in cars driven predominantly at low speed for short distances, i.e., in cities (Spreen, 2016). According to a recent Dutch TNO report vehicle owners frequently choose to have the filter removed, since replacement of a clogged DPF can be very expensive. When a DPF is physically removed (or drilled), the DPF software routines (‘chip tuning’) are also removed from the vehicle’s engine management system or pressure sensor emulators are used to make the OBD system believe that a fully functioning DPF is still present. As such, a removed DPF goes unnoticed during the OBD fault code check, performed a part of the I/M test. This may, however, occur less frequently in regions where vehicle have mandatory inspections with tailpipe measurements.

For these reasons the European Commission is currently tackling the above situation by exploring possible measures, legal and technical solutions to strengthen the anti-tampering with the exhaust emission control system enforcement within the roadworthiness-framework. It is stressed that these discussions take place in parallel with the discussion on mileage fraud and solutions that are being considered in one case can be of interest to the other.

Ultimately a vision for DIAS is to be perceived as the Swiss border police checking each vehicle continuously and meticulously but without this physical effort at the border.

1.2. Objectives

The overall objective of DIAS is to support the transition to more effective protection and detection systems based on OBD/OBM that will ensure a strong reduction of the tampering activities. The project aims at defining methods and providing a solid basis for future standards in the security and diagnostic systems to ensure that hardware, software and communication manipulation will be detected and that the detection will be successful regardless if the manipulation attempt has been foreseen or not during the initial design of the system. At the same time, DIAS will pay particular attention to the accuracy and security of emission performance data reported by on-board vehicle electronics to enable use of these data in environmental policies such as pay-as-you-pollute schemes.

DIAS aims at achieving a strong reduction or total elimination of tampering emissions-relevant systems by means of high resistance to hardware and software manipulation and detection of tampering. This will be demonstrated by independent teams by implanting tampering devices for different emissions control systems and subsequent verification of their detection by vehicle monitoring systems in laboratory test conditions as well as in real driving.

This overall target is broken down into four main objectives as follows:

I. “Market” analysis and assessment of the operation of representative tampering systems and of their effect on the performance of existing on-board emission monitoring and emission control systems over real-world and laboratory testing. (WP3)

- In achieving this objective, an inventory of device providers is compiled through market research; it enables the assessment of the overall dimension of what is being offered as cheating devices.
- Cheating devices are categorized in terms of principle of operation and weaknesses of existing systems that tampering devices exploit.
- Risk assessment is performed for the potential of tampering separately for light and heavy duty vehicles (as well as Non Road Mobile Machinery) and the corresponding emission-control system, with focus on de-NOx systems of heavy-duty vehicles and particulate filters on all vehicles.
- Quantified Target:
- A matrix of tampering challenges is compiled with representative cheating devices selected from each category. This matrix is used to evaluate existing vehicle diagnostics as well as the advanced ones developed within the project. The matrix contains at least three representative variants of each tampering system category.

II. Detection methods and counter-measures are identified and implemented (in vehicles) (WP3, 4, 5)

- The tampering devices are tested in the laboratory to understand their principle of operation and to decide if they are to be installed and tested in a vehicle.
- Selected tampering equipment is installed on vehicles to demonstrate the effect of manipulation under real world conditions and generate sufficient data signals for the analysis of the device operation.
- Hardening of EPS is achieved: Tampering attempts provided by WP3 through software or hardware modification are prevented or detected in case that an intrusion cannot be effectively prevented by system security solutions only
- Future tampering attempts are prevented or detected by an advanced anomaly detection system. Future-proof the measures by also approaching this challenge with the most modern technologies available (secure hardware, verifiable software, Internet-of-Things (IoT), and anomaly detection) that offer the needed flexibility and dynamics to always keep one step ahead of the tampering threats.
- All developed concepts and architectures including prototype ECU, CCU and a cloud-based system integrated to a demonstrator vehicle

Quantified Target:

- At least one demonstrator vehicle equipped with enhanced tamper-proofing measures, software and electronic component security systems.

III. Testing and demonstration of the success of measures

- The capability of diagnostic systems to detect tampering methods and maintenance issues is assessed for light and heavy-duty vehicles by means of independent testing including real driving conditions.
- The demonstrator as described in objective II is built containing the future counter-measures from objective II (ECU, Communications Control Unit (CCU), Cloud) including software and communication security features.

Quantified Target:

- The demonstrator vehicle is proven to be able to detect the tampering challenges contained in the matrix developed by means of an evaluation by independent security experts as well as within an open competition organized within the project (Hackathon). For this event ethical hackers are invited to hack the system in order to find vulnerabilities that can be exploited to manipulate the emissions control system of the vehicle.

IV. Setup of guidelines and recommendations for future legislation for the introduction of future safe monitoring systems (WP 6).

- The knowledge gained in the testing of tampering devices, and in the development of antitampering measures is leveraged to recommend regulatory provisions that prevent misinterpretation and regulation beating.
- The proposals are reviewed by several stakeholders including the advisory board, the associated industry as well as drivers' and consumers' associations.

Quantified Target:

- Regulatory proposals made in a uniform and technology-neutral way.

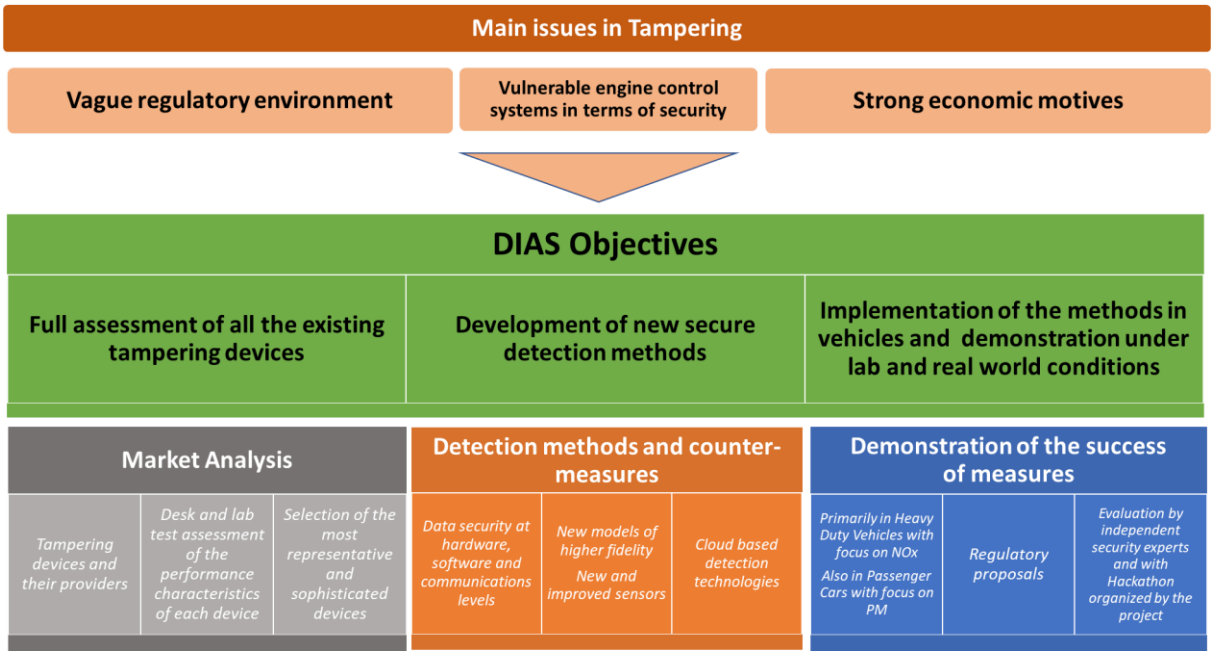

Fig. 1. A graphical illustration of the project

2. Concept and methodology

2.1. Concept

DIAS will be based on a two-step approach that is represented by three levels in Fig. *2* conceptually illustrates how the DIAS project will coordinate its activities from the bottom left corner measures to the top right corner measures. This starts with the current tampering approaches that can easily work around standard OBD as indicated in base level (level 0).

Level 1 builds on conventional OBD in the base level (level 0) and level 2 builds in turn on level 1 in order to achieve the ultimate capability for prevention and detection.

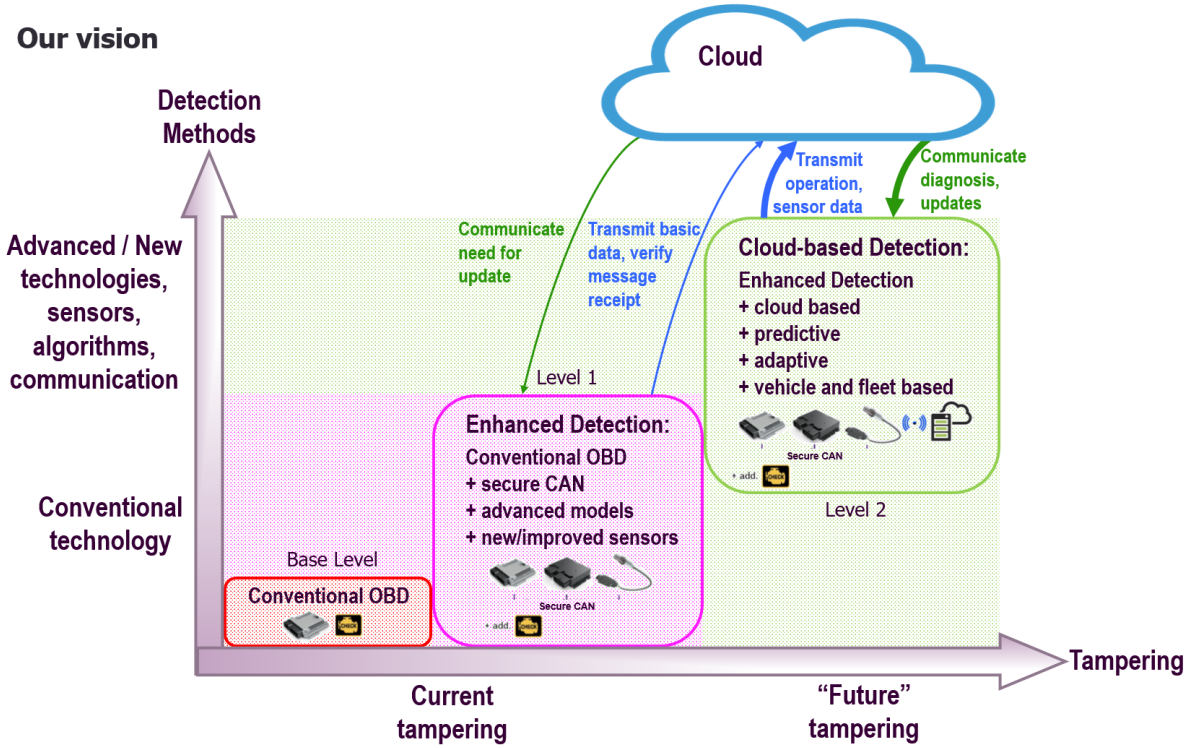

Fig. 2. DIAS main concept

2.1.1. Base level: identification and assessment of current status

Vehicles currently in market are continuously monitored by their OBD system to ensure proper functionality of components and systems to set a trouble code and inform that driver if a malfunction is discovered. By design, since OBD monitors the rationality of various physical (e.g. temperatures, pressures) and derivative (e.g. EGR rate, calculated flowrates) quantities, it is in the position to detect certain tampering attempts that may affect signals already being monitored for purposes other than tampering but may be affected by tampering systems. Therefore, it inherently contains some functionality to assist tampering detection although not designed to cope with such malicious interventions. In addition, as emission standards get more stringent, OBD systems get more complex and more engine and vehicle operation related quantities are being monitored against more advanced algorithms and reference signals making tampering even harder since more reference signals may be incidentally affected by a tampering exercise and therefore trigger a malfunction indication in the engine electronics.

DIAS will take advantage of this inherent antitampering functionality of OBD systems and begin with a holistic market analysis to identify tampering techniques and equipment and the capability of current OBD systems to detect these tampering methods as well as the way this is achieved. It will define the link between different levels of manipulation (vehicle system internal communication and electronics in general, physical modifications of hardware etc.) and the ability of OBD to detect them. This link will be explored in relation to the emission standard of vehicles (as already mentioned Euro VI vehicles are more difficult to tamper compared to Euro V vehicles) as well as in relation to different diagnostic concepts and technologies employed by each OEM. This will allow, on one hand, to determine the capability of existing vehicles to detect tampering and, on the other hand, identify the way and intrusion points existing tampering systems exploit to achieve emission control systems manipulation without affecting signals that are incidentally monitored by the OBD system.

As a result of this exercise, the architecture and operation of existing tampering systems in real world operation and by in-depth in-lab analysis and will be categorized in groups of similar approaches. This analysis will identify what is missing from current OBD to be further enhanced to achieve tampering detection as well. Furthermore, the analysis will allow to make scenarios of what is expected to be introduced in the market as future tampering methods and therefore define the challenges to be address within DIAS. The boundary conditions to determine when any possible future tampering method has been covered in the list of DIAS is cost. Any kind of manipulation is possible, for instance complete replacement of vehicle electronic control systems. It is not necessary though for

antitampering systems to be able to detect such exercises since they would be too expensive to implement and therefore not of interest to vehicle users.

2.1.2. Level 1: measures for enhanced detection using conventional techniques

A development based on the implementation all possible improvements already available or at advanced development level to the existing on-board detection logic. Level 1 approach will include measures such as secure vehicle internal communications (secure CAN), increased number of plausibility checks in engine and aftertreatment control control-related quantities (e.g. exhaust temperature), advanced emission and operation prediction models, advanced virtual and hardware sensors, revised on-board electronics with increased processing power etc. It will also be used to gain the first experience with the cloud. In particular, it will be possible to store data in the cloud, using distributed ledger technology such as block-chain, that cannot be manipulated and always available for future reference (comparisons/calculations). Data that could be quite valuable here are based on examples of SCR emulators the frequency of clearing the fault code memory that tampering approaches must often reset in order to remain undetected. If a high frequency is observed and documented, then it indicates that tampering may be taking place and needs to be checked more carefully and is used as one input to contribute to the calculation of the tampering probability by the detection algorithms.

Although level 1 measures are not expected to suppress all tampering methods, according to the expertise of the consortium they are expected to render useless tampering systems that are less advanced, require limited installation skills and are of low cost. The target is to develop measures that raise the tampering effort just enough to wipe out all the cheap low-end offerings, just to reduce the playing field, and start preparations for more advanced antitampering architectures.

Level 1 measures will, on one hand, have the advantage of being more robust conventional systems providing a framework for less demanding requirements that can be implemented in intermediate regulatory steps. On the other hand, since these approaches will require low lead time for implementation they will have a faster impact on the reduction of tampering and consequently emission saving. Level 1 will demonstrate the weaknesses not possible to be addressed by this conventional approach and provide input to design the a more advanced architecture to allow complete resolution of any possible future tampering methods that may appear in the market.

2.1.3. Level 2: measures for cloud-based adaptive detection

The second level will utilize the full potential of connection to the cloud. This encompasses both the storage of data that cannot be manipulated (in the cloud) and the computational capabilities that will be valuable for anomaly detection as described later in the section on methodology.

The main advantages and content of the ECU-CCU-Cloud based concept as shown above in level 2 are:

- In case of new or changed tampering strategies appearing on the market, new diagnostic modules can be developed based on the analysis of new behaviour of the threats. These modules can be downloaded (deployed) into the CCU and executed to provide new addition information or features for tampering detection. One major advantage of functions available locally in the control units is that this method is also applicable for vehicles which are already in the field. In addition, specific data sequences based on system signals can be requested and sent to the cloud for further analysis, e.g. by pattern recognition algorithms, for short term and long-term observation of the vehicle and data behaviour. An additional benefit of using the CCU is that ECU data does not need to be changed and thus being not subject to new emission type approval.
- Signals and features from the ECUs and the CCU will be sent to the cloud for further post processing. The cloud offers the opportunity to combine signals from different vehicles in the field and to combine them with e.g. environmental data. In addition, experts can be included in the analysis and can requested data to be additionally used for plausibility/tamper detection if needed. As already describe above it is also possible to react flexibly to new threats due to the development of adapted modules.
- As the major analysis is done in the cloud it already offers a high degree of security against local systems in the vehicle (a neutral observer that cannot be bribed)
- The cloud offers an initial tampering detection of potentially tampered and suspicious vehicles based on the diagnostic decision. In addition, also the activation of the inducement system might be activated.

The concept of combining the cloud capabilities with the engine management system and after-treatment controls and sensors is shown as an example in the following system overview, Fig. 3, below. The figure represents a standard two-box (referring to the control units Engine and Dosing-Control unit) environmental protection system (EPS) with sensors that have both digital (SCU-Sensor Control Unit) and analog interfaces with the ECU/DCU.

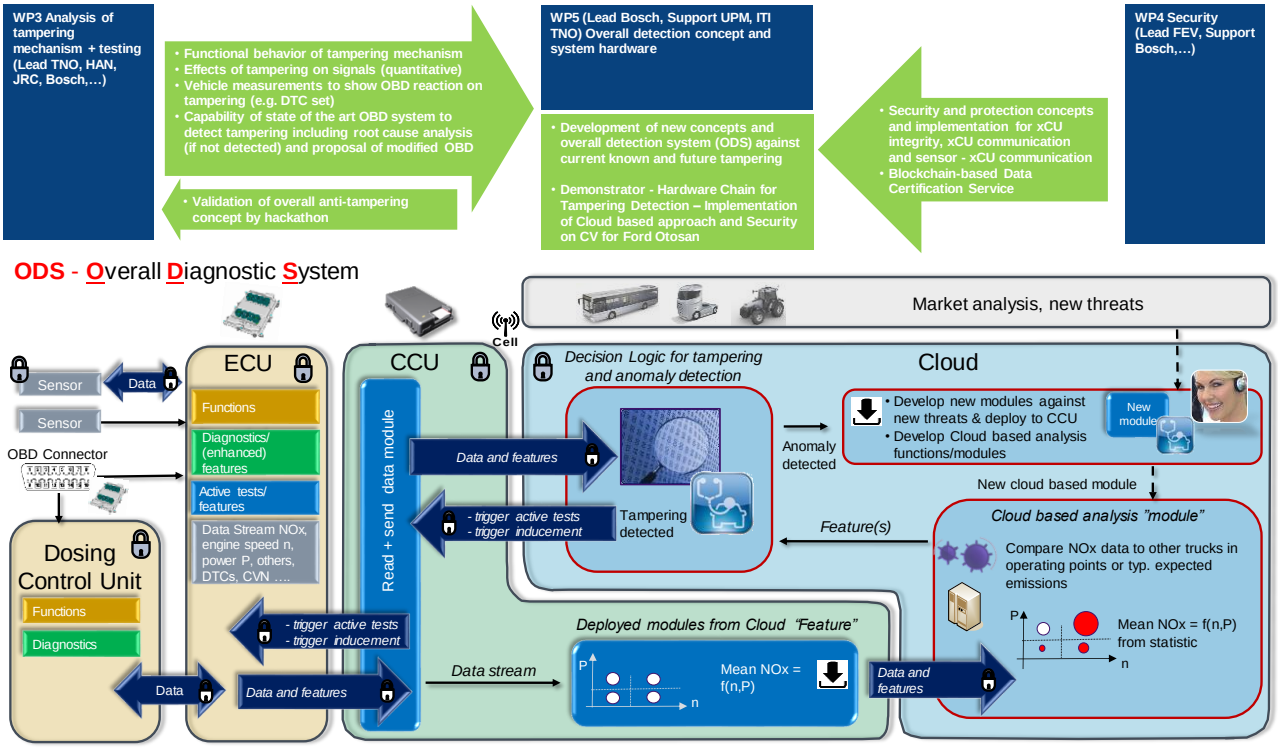

Fig. 3. DIAS architecture

The advanced diagnostic system will utilize the full potential of future connected vehicles. On the one hand there are extensive opportunities due to intelligent solutions made possible by data available and computational power in the cloud, but on the other hand connecting vehicles means new risks due to increased entry points into the vehicle's control systems. The DIAS approach is based on a concept to monitor the performance and status of vehicle emission control systems and compare it to a historical performance (and status) not susceptible to manipulation by utilizing these technologies. In particular, DIAS concept proposes to monitor vehicle operations in an aggregated form in order to generate reference indexes resulting from combination of signals that the vehicles can use in turn to detect tampering attempts and implement measures to inhibit these attempts, under diverse conditions anticipated in real world operation, independent of vehicle usage (traffic, load, road slope etc.).

The targeted robust system will base its architecture on the fact that any manipulation attempt will have an influence on vehicle operation parameters. For instance, flashing of the ECU for power increase will increase the performance of the vehicle outside of existing engine and vehicle maps. If a tampering effort aims at reducing fuel consumption, this will be reflected in the actual fuel consumption of the vehicle. Non-replacement of faulty vehicle components but masking of the detection of a failing component will result in registration of such event if replacement is expected according to advanced part ageing prediction techniques. It is assumed the attempt will aim at increasing vehicle emissions without any benefit to the user.

Therefore, what is needed is an independent observer (at "home" in the cloud) that will monitor vehicle operation and maintenance and which will be impossible to be manipulated or muted by the user. In addition, since existing modelling techniques are not able to simulate each expected operation, data should be evaluated at fleet level (big data collection and processing) to allow also advanced anomaly detection techniques to be deployed. For all these reasons, this independent observer should be a central system to which all data are communicated and no vehicle user has access and therefore the opportunity to manipulate. This central system will be in the position to process collected data, generate reference signals and data and detect tampering attempts, distinguishing them at the same time from normal vehicle operation including particular ones such as extreme driving and climatic conditions, normal vehicle degradation etc. Furthermore, the system should be able to deploy updates in existing software or

injection of specific data collection modules to vehicles in the field whenever this is considered necessary.

What is required on the vehicle end is communication and hardware safety to prohibit any data manipulation that would introduce instability and errors to the data collection system. In case this would happen, the independent central system will be able to detect it, especially if it happens at a significantly wide range in the field. In addition, any attempt to stop communication of the vehicle to infrastructure or the remote installation of necessary updates will activate on-board inducement strategies to force the driver to reverse manipulation or solve the problem without the need of law enforcement intervention.

The operation of these systems in the cloud will be in the responsibility of the OEM which can be purchased as a service from a supplier in case this is considered more efficient by the OEM. Bringing the operation of these systems to the community by means of standardized interfaces will ensure technology neutral implementation allowing at the same time the integration of the advanced diagnostic systems to the existing vehicle infrastructure in a holistic approach. The latter will minimize the societal cost due to the possibility given to the OEMs and suppliers to implement systems using their most convenient and cost friendly solutions due to the possibility to leverage scale-economies. Cost will be further reduced by the possibility given for the formation of alliances and clusters of OEMs or even suppliers.

Data from these systems will be ensured to be made available to authorities, policy makers, and environmental bodies in a reliable and undisputable way. This is imperative since such data may likely be used for taxation and other schemes (e.g. pay-as-you-pollute). However, in such cases there is a perverse incentive since the community will benefit from falsified reporting of lower emissions. One way to introduce this is by in-service conformity testing where test data will be compared with data on the cloud.

2.2. Methodology

The project will cover a variety of activities designed to define and demonstrate the best available technology (BAT) and to provide guidelines for legislation (WP6). It will be based on the four main pillars.

- Pillar a. includes system analysis to identify the way existing tampering systems operate, foresee possible threats that will emerge in the future and set targets for the diagnostic systems to be developed within DIAS (WP3).
- Pillar b. includes security at the three levels of data flow, i.e. hardware, software and communications, the challenges in these fields and the available technologies to cope with these challenges (WP4).
- Pillar c. includes monitoring of vehicles and the application of sensors for direct assessment of operation and performance as well as storage, transmission and handling of the collected data.
- Pillar d. includes diagnostics. As discussed above, these are distinguished in: (i) on-board – based on existing conventional approaches; (ii) remote – based on fixed stationary diagnostic systems; and (iii) as remote adaptive – based on stationary infrastructure-based diagnostic systems. The latter can adapt their diagnostic strategies using either the collected data at vehicle and fleet levels as well as market and in-field information (WP5).

3. Expected results

The project will provide impact assessment calculations and comprehensive information on the emission benefit expected from the adoption of the proposed highly efficient diagnostic and antitampering systems for timely detection of malfunctions and emission reduction system manipulation. Test data will be complemented with OBD emissions' and general emissions' models, available in-house to provide estimates in mass of pollutant saved per fleet and per km, as well as the cost effectiveness of such systems for different implementation scenarios.

Complete diagnostic systems will be proposed ranging from highly optimized OBD/OBM systems with an intelligent combination of signals and new models, up to cloud-based solutions. The latter will draw upon data-to-infrastructure communication integrity technologies with advanced cryptographic primitives, such as blockchain, as well as solutions for anomaly detection, both vehicle and fleet based. These are expected to guarantee the targeted extremely high resistance to tampering for uninterrupted detection of malfunctions during the lifetime of the vehicle, eliminating possible future threats.

A final step of the project will be to validate the proposed systems by verifying their diagnostic efficiency under specific test and tampering inducement protocols, in the lab and in real-world.

All proposed methods are possible to be described in legislative text to be implemented in a uniform and technology-neutral way. One important element that will be considered is not to allow room for misinterpretation and regulation beating techniques. For this reason, the final proposals will also be submitted for peer review to several stakeholders including the advisory board, the associated industry as well as drivers' and consumers' associations.

Acknowledgements

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

References

European Commission DG Move, 2017. Discussion on tampering with the exhaust emission control system, point 4 of the Summary Report
of the Roadworthiness Committee meeting, held on December 4.

Pöhler D., Adler T., Krufczik C., Horbanski M., Lampel Johannes., Platt U., 2017. Real Driving NOx Emissions of European Trucks and
Detection of Manipulated Emission Systems, 19th EGU General Assembly, EGU2017, proceedings from the conference held 23-28 April, 2017 in Vienna, Austria., p.13991.

Spreen J. S., Kadijk G., Mark, P. J., 2016. Diesel particulate filters for light-duty vehicles: operation, maintenance, repair, and inspection, TNO
Report R10958.

Switzerland, 2017. Manipulations on EURO V and VI trucks by suppression of AdBlue injection - Status report from Swiss heavy-duty truck
controls, Informal document WP.29-172-28, 20-23 June 2017, submitted by the representative of Switzerland.

United Nations Economic Commission for Europe, 2018. Tampering of Air Emission Control Systems, IWG on Periodical Technical Inspections, Informal document WP.29-175-07, 175th WP.29, 19 - 22 June 2018 Agenda item 8.1., https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29/WP29-175-07e.pdf