DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D3.3
Deliverable Title	Implementation of anti-tampering measures into the existing legislative framework
Issue Date	29/11/2022
Dissemination level	Public
Main Author(s)	Iddo Riemersma (TNO) Robin Vermeulen (TNO)
Version	V2.0

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
Draft	Draft versions	TNO internal content review	Reviewer: Ann Delahaye, Robin Vermeulen (each others content)	23/09/22
v0.2	Draft content of deliverable	Content review	LAT ICCT	11/10/22
V0.3	GA check	Content review	All partners	20/10/22
V1.0	Final content	-	-	16/11/22
V2.0	Revised final content		Revision asked by EU officer	

Verification and approval of final version

Description	Name	Date
Verification of the “Draft final content of deliverable (v0.3)” by WP leader	Ann Delahaye (TNO)	14/11/2022
Verification of the “Final content of deliverable v1.0” by the coordinator	Zissis Samaras	16/11/2022
Verification of the “Revised final content of deliverable v2.0” by the coordinator	Zissis Samaras	29/11/2022

Executive summary

Pollutant emissions from road vehicles have reduced significantly thanks to the development and application of effective and often sophisticated emissions control systems. Tampering of these systems leads to elevated emissions comparable to uncontrolled levels of vehicles of decades ago. Therefore, a small share of tampering potentially leads to a significant increase of the EU fleet average emissions.

The DIAS project focused on developing and providing technical solutions for tampering prevention, detection and reporting. It is important that solutions are effectively implemented on new vehicles so as to ensure that these prevent, or detect and report possible tampering as good as possible during the lifetime of a vehicle. The original goal of Task 3.3 was to develop a test protocol to be used at type approval to check the effective implementation of technical solutions. This presumes that adding a test protocol is the best solution for implementation into the type approval procedure. However, during the execution of the DIAS work it became clear that this may not be the most effective way to ensure that effective anti-tampering measures are taken for vehicles entering the EU market. A test protocol is fixed and predictive, while tampering strategies tend to explore new angles that may bypass any test protocol. Fixed testing protocols limit the scope and thus the performance of a system to what is exactly tested and testing burden will be high when the tested system is complex.

Instead, a broader perspective has been followed by developing guidelines for the legislative framework, taking a more holistic approach from which the guiding principles and criteria for implementing the required anti-tampering measures will follow and which is based on setting functional requirements for new vehicles and vehicles in-service. This approach is assumed to be more effective in the prevention, detection and reporting of tampering, not only for new vehicles but also during the lifetime of a vehicle.

Based on the technical solutions that were developed in DIAS, functional requirements have been defined which form the basis for the approach. A functional requirement means that the objective of the legislative requirement is described in qualitative terms of what 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 it is stimulated to apply the most cost-effective anti-tampering solution. Relative technical details, where needed, are documented only as technical examples and along with regulations to be amended. Because tampering is often developed by exploiting vulnerabilities of vehicles in-service with public road admission, it is recommended to not only define functional requirements for new vehicles but also for vehicles in-service.

Concluding, the proposed requirements for OEMs (also integrating the role of the Type Approval Authority (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 based on the following steps:

- 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
- 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.
- Provide tampering-related and secure methods for in-vehicle and V2I reporting.
- Develop methods for inducement and enforcement of repair.
- 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:

- General statement on tampering prevention
- Proactive monitoring of vehicle fleet
- Allow third party to supply tampering evidence

Contents

Executive summary **4**

1 Introduction **7**

1.1 Background 7

1.2 Objectives and approach 7

1.3 Deliverable structure 7

1.4 Deviations from original DoW 7

2 Approaches to ensure conformity with OEMs' anti-tampering requirements **9**

2.1 Original approach 9

2.2 Proposed approach 9

3 Conclusions **12**

1 Introduction

1.1 Background

The DIAS project has led to a set of requirements (DIAS Deliverable D6.5) for the detection of tampering by improved vehicle internal diagnostics, enhanced vehicle security features and for reporting of relevant tampering data from the vehicle to a cloud. To become effective, they will need to be formalised in one way or the other. Implementation of these recommendations is thought to take place as an add-on to the existing vehicle emission legislation within the vehicle EU type approval framework (i.e. EU regulation 2018/858 (European Parliament, Council of the European Union, 2018).

Originally, the objective for Task 3.3 was described as "Definition of a practical test protocol for testing for future Type approval testing of system hardening against tampering and tampering detection, based on requirements set in WP2 and testing experience in WP3". Instead of developing a test protocol, it was decided that it would be better to take a more holistic approach from which the guiding principles and criteria for implementing the required anti-tampering measures will follow. As a result, the objective has been redefined. It was also decided to incorporate the outcome of Task 3.3 to DIAS Deliverable 6.5 *Guidelines, impact assessments and text for future legislation*. In this way, the DIAS recommendations for a future anti-tampering framework are described in a single document. This deliverable (D3.3) will therefore report on the change of objectives and work, and provide a summary of the outcomes of Task 3.3.

1.2 Objectives and approach

Given the insights as obtained during the project, the new objective of Task 3.3 was to investigate and provide the guiding principles that can be used to ensure the implementation of effective countermeasures which are needed to prevent or detect and report tampering with the vehicle emissions control system, not only when new vehicles enter the road, but also during the lifetime of the vehicle.

The starting point was formed by the guidelines and recommendations reported in Deliverable 6.5 as an outcome of this project. The next step was to determine which legislative options exist to implement these as requirements into the existing vehicle type approval legislation. By focusing on the objective, it was evaluated what the most effective strategies are, leading to the recommendations for the implementation of the requirements into legislation.

1.3 Deliverable structure

This deliverable is organised into three chapters:

- Chapter 1 provides the background, change of the objectives and the description of work (DoW), and structure of this deliverable.
- Chapter 2 evaluates the approaches to ensure conformity with the legislative requirements.
- Chapter 3 concludes the purposes and summarises the findings of this report.

1.4 Deviations from original DoW

1.4.1 Description of work related to deliverable as given in DoW

In the DoW, the description of the Task 3.3 in *Grant Agreement-814951-DIAS (p97)* is the following:

Task 3.3: Type-approval test protocol for legislative context.

Definition of a practical test protocol for testing for future Type-approval testing of system hardening against tampering and tampering detection, based on requirements set in WP2 and testing experience in WP3.

A test protocol will be drafted that can be used in a legislative context, i.e. in the framework of the EU type-approval system for vehicles and engine systems. General criteria will be set for the test protocol. Early in the project experience with the tampering techniques and testing will be combined to draft a procedure that can be implemented in the EU type-approval scheme. Taking into consideration the legislative process of development of new test procedures, the stakeholders will be consulted to discuss the practicability of the procedure and adjusted if needed.

The final test protocol is validated on a LD and a HD vehicle. A golden engineer will execute the draft test protocol and it will be validated whether the test procedure fulfils the criteria as initially set.

In the DoW, the description of the Deliverable D3.3 in *Grant Agreement-814951-DIAS (p100)* is the following:

D3.3: Anti-tampering test protocol for use in future type approval test: A report on the test protocol to be used in a legislative context

1.4.2 Time deviations from original DoW

This work has been executed in accordance with the project planning.

1.4.3 Content deviations from original DoW

According to the original DoW, a test protocol should be drafted in a legislative context. This presumes that adding a test protocol is the best solution for implementation into the type approval procedure. However, during the execution of the DIAS work, it became clear that this may not be the most effective way to ensure that effective anti-tampering measures are taken for vehicles entering the EU market. A test protocol is fixed and predictive while tampering strategies tend to explore new angles that may bypass any test protocol. Instead of the task description in §1.4.1, a broader perspective has been followed by developing guidelines for the legislative framework, taking account of the need to have anti-tampering measures implemented on new vehicles. This approach is assumed to be more effective in the prevention, detection and reporting of tampering, not only for new vehicles but also during the lifetime of a vehicle. The guidelines for the framework therefore consider requirements for Type-Approval for new vehicles and for vehicles in service. This approach could fit a possible future anti-tampering framework within the EU emissions legislation with roles for OEMs, Type-Approval Authorities, Market Surveillance authorities and third parties. Because of this deviation the title of the report was changed from *Type-approval test protocol for legislative context* to *Implementation of anti-tampering measures into the existing legislative framework*.

2 Approaches to ensure conformity with OEMs' anti-tampering requirements

2.1 Original approach

The initial approach to ensure conformity with anti-tampering requirements addressed to OEMs was to define a practical test protocol for future Type approval based on the tampering market analysis, risk assessment and testing experience conducted in the first period of the DIAS project. The current automotive vehicle emissions type approval regulation in force over the European Union (EU), already includes requirements for testing conformity with other legislative requirements. For example, EU and United Nations Economic Commission for Europe (UNECE) vehicle emissions-related legislation requests tests to demonstrate compliance with the OBD requirements based on specific failure modes to be tested. The advantage of using testing protocols embodied with specified technical requirements is that the responsibilities of the OEMs are clearly set and compliance is independent of interpretation. Even if this is a straightforward approach seeming to avoid the loopholes in the regulation that can be exploited, there are still some significant aspects limiting the effectiveness of such type of regulation on mitigating tampering with vehicles' EPS. To further and properly investigate these limitations and arrive at the best approach to follow in the future type approval, the corresponding work (i.e. Task 3.3) of this deliverable was significantly extended, time-wise, and carried out throughout the whole period of the DIAS project (included in the amendment of the Grant Agreement).

As observed from the tampering market analysis and testing activities during the early stages of the project and documented in deliverables (D2.1, 2020), (D2.2, 2020), (D3.1, 2020), (D3.2, 2020) and (D4.1, 2020), each tampering device or service is tailored to a specific vehicle model and many variations are available to cover the vehicle fleet. Assuming a similar approach as the current OBD tests (i.e. testing the conformity by the introduction of specific failure modes), the TA test protocol should include several tests to be applicable to all vehicles.

At the same time, an enhanced anti-tampering testing protocol for future type approval should aim to ensure that vehicles are protected against the (most critical) tampering threats, proportional to the risk analysis performed during the drafting of the regulation. This means that vehicles granted type approval will be protected against currently known critical tampering threats. Even though the main effort of tampering market analysis and risk assessment was allocated to the first year of the project, regular monitoring of the tampering market was conducted by all the DIAS partners during the whole project duration (i.e. 3 years up to the end of October of 2022) to evaluate and update the market analysis results. Consequently, new valuable input, ideas and questions were introduced revealing that the tampering market is changing constantly, needing continuous monitoring and (re-)evaluation. In short, it was concluded that not all possible -current and future - tampering strategies are known and can be reasonably identified. Therefore, legislation that sets specific requirements and testing towards anti-tampering will eventually become outdated. Then, several amendments would be needed to cover the new threats. Such an arms race is not considered an efficient approach for the type approval legislation.

2.2 Proposed approach

The work of Task 3.3 is reported in DIAS Deliverable D6.5, in chapters 3 and 4. A short summary with additional details of the work outlined in that deliverable is provided here.

Before providing the guidelines of the legislation framework, it should be recognised that a vehicle can never be made completely tamper-proof because with sufficient budget and effort any system can be

hacked. Therefore, tamper prevention detection and reporting should be such that it is simply not cost-effective to develop and apply any tampering solution.

Another important element is that tampering can be done in different ways and new angles for tampering may be explored and developed that have not yet been identified before. From that point of view, it is preferable to specify requirements in a functional way, i.e. describing what is the desired outcome from the anti-tampering system. This is in contrast to setting technical requirements, which only describe what the system should fulfil in terms of characteristics, (emission) standards, and/or (test)protocols with specific measurable criteria. Though technical requirements may have a supporting role to counteract foreseeable tampering strategies, they are not sufficiently flexible and need regular updates to keep their relevancy.

The recommended approach for the implementation of anti-tampering into the legislation is two-fold, with an ex-ante and an ex-post element.

2.2.1 Ex-ante approach

Within the existing emissions type approval, new functional requirements are included for the development of specific countermeasures for vulnerabilities that can be foreseen. This is implemented in the following steps, to be performed by the OEM:

- Perform a risk assessment and market analysis to address all known and foreseeable tampering strategies (TARA: Threat Analysis and Risk Assessment)
- Apply fundamental countermeasures to address known tampering strategies and develop dedicated countermeasures to address any foreseeable tampering strategies, based on the TARA.
- Provide tampering-related and secure in-vehicle and/or vehicle-to-infrastructure reporting.
- Implement vehicle inducement strategies to enforce repair and maintenance.

A declaration of conformity to these legislative requirements could be required, together with the obligation to deliver an information package on the applied countermeasures. The Type Approval Authority (TAA) could be given the mandate to ask for dedicated demonstration tests, tailored to the specific technologies of the emission control system applied, including the functioning of the in-vehicle reporting (tampering indicator, MIL) in the case that tampering is detected by the vehicle. For such demonstration tests, there are no pre-defined test procedures in place.

It should be noted that the fundamental countermeasures could be regularly updated. For example, to ensure a kind of updatable regulation, the EC occasionally assigns expert groups to periodically provide and update requirements-related lists and then, 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 approval authorities and this list is made available to the public by the EC (European Parliament, Council of the European Union, 2019). Similar methods could be adopted to regulate an updatable list with the known tampering methods and potentially the fundamental tampering protection and prevention countermeasures.

Consequently, OEMs could deliver two different information packages for each type of countermeasures implemented:

a. Information package containing the list of known tampering methods and the technical countermeasures applied to address these threats in terms of prevention and detection.

b. Information package containing the list of tampering methods based on the TARA and market analysis, and finally the technical countermeasures applied to address these threats in terms of prevention and detection.

2.2.2 Ex-post approach

The ex-post approach comprises any element that supports monitoring of in-service vehicles' compliance against new tampering strategies. In this case, several entities are involved including OEMs, TAA, EU Member States (MS), roadworthiness inspection and other authorities.

The basic approach is that by means of monitoring the manufacturer, in collaboration with the TAA but also other National Authorities (such as ISC or MaS), could monitor 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. This should lead to a cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating threats, and developing updates for the countermeasures and the inducement of vehicles (vulnerability management). In the case that tampering activities are observed by the OEM, third parties or MaS, the type approval authority 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 and the investigation is publicly reported. Based on the outcome of this investigation, the manufacturer may be required to take appropriate countermeasures based on an impact assessment. These 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 maybe not be enough to install resource-demanding diagnostic or security solutions.

Vulnerability management is essential for dealing with potential new tampering strategies and is meant to ensure that possible newly found vulnerabilities are resolved, either on the vehicles in service or on the next generation of vehicles entering the market.

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

3 Conclusions

Based on the tampering market analysis, risk assessment and testing experience conducted during the duration of the DIAS project, it was shown that a practical test protocol for future type approval cannot protect vehicles against critical tampering threats due to the continuous evolvement of the tampering market. Thus, a test protocol is not seen as the most effective option to ensure conformity with OEMs' anti-tampering requirements.

An alternative approach was proposed that could ensure that anti-tampering provisions applied by OEMs are effectively implemented not only on new vehicles but also during the vehicle's useful life. The approach is largely based on setting functional requirements instead of testing protocols. The suggested implementation distinguishes two elements:

For the type approval of new vehicles: functional requirements for the development and implementation of specific countermeasures for vulnerabilities that can be foreseen. This includes Threat Analysis and Risk Assessment (TARA), prevention and detection countermeasures, tampering-related and secure reporting, inducement and enforcement of repair, demonstration and declaration of conformity with legislative requirements

For vehicles in service: functional requirements that force the OEM to follow up on signs from the market that tampering might be taking place. Vulnerabilities are managed 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). To this end, a general statement on tampering prevention is included, requiring proactive monitoring of vehicle fleet using input from various sources such as the tampering detection and reporting, allowing third parties to supply tampering evidence, supplemented by an enforcement regime and a review clause.