DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D1.1
Deliverable Title	DIAS Project Handbook–inception version
Issue Date	29/05/2020
Dissemination level	Public
Main Author(s)	Dimitrios Kontses (LAT/AUTh)
Version	V2

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	Reviewer: Savas Geivanidis (LAT/AUTh)	
V0.2	Draft content of deliverable	Content review	Reviewer: Savas Geivanidis (LAT/AUTh)	
V0.3	Final content of deliverable	Content review	Reviewers: Ann Delahaye, Andreas Hastall, Obaid Ur-Rehman	
V0.4	Final content of deliverable	Verification	All partner managers	
V1.0	First final version	-	-	-
V2.0	Update for publications and templates for documents ("live" document)	-	-	-

Verification and approval of final version

Description	Name	Date
Verification of the "Final content of deliverable (v0.4)" by WP leader	Savas Geivanidis (LAT/AUTh)	
Check of the "First final version (v1.0)" before uploading by coordinator	Zissis Samaras (LAT/AUTh)	

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background of DIAS

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. 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, 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 are at least 100 companies worldwide (mainly in Europe but also from China) offering kits for purchase with prices ranging from 10 to 500 €.

A German study on emissions by trucks showed that one in every four trucks from Eastern Europe showed NO_X emissions much higher than the EURO norm, which implied manipulated emission systems (Pöhler et al., 2017). Reports by Swiss authorities showed that in Switzerland only Euro V compliant vehicles were caught with basically in-hardware manipulations, which include emulators and simple built-in potentiometers that stop the dosage of the reagent AdBlue™ (used in SCR systems for the reduction of NOx emissions) (unece.org, 2018). Professional manipulation of Euro VI systems seems to be more difficult and probably 10 times more expensive compared to Euro V. In the UK, about 8% of the lorries tested across the country were found with an emission control cheating device (AECC, 2018).

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, Kadijk, & Van der Mark, 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 (exact source). 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. In a system, tampered this way, 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.

The overall objective of DIAS is to support the transition to more effective protection and detection systems based on On-Board Diagnostics and On-Board Monitoring (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 countermeasures 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 prevent or detect the tampering challenges contained in the matrix developed in WP3. Effectiveness is judged within open competitions organized within the project (Hackathons). For these events 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. There will be two hacking events. Many details for these events will be provided in a next deliverable but briefly:
    - 1st Hackathon: Focussing on in vehicle measures like secure communication and improved OBD.
    - 2nd Hackathon: Additionally, the connectivity infrastructure will be tested.

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.

1.2 Purpose of the document

The purpose of this Project Handbook is to describe the procedures and processes that are generic for all Work Packages and that enable smooth cooperation. Also, it contains a more detailed plan for the work packages and the progress within each work package.

According to the workplan, this document constitutes Deliverable 1.1 and it is submitted to the Commission via the Research Participant Portal.

1.3 Document structure

Chapter 1 contains the introduction of the deliverable including the purpose, structure and deviations from the DoA (Description of Actions).

Chapter 2 below describes the management structures, including the nominees for the various boards.

Chapter 3 is dedicated to specific quality management procedures, including communication structures and tools, the peer reviewing process for high quality deliverables, as well as risk management and other quality assurance means.

In Chapter 4 the technical infrastructure for communication and collaboration is presented.

Chapter 5 outlines the specific ethical guidelines that the project is following.

In Chapter 6 the consortium's strategy towards openness is described and relates to open source in terms of software as well as open access in terms of publications and other project results.

The Annex includes an example of template used throughout the project.

1.4 Deviations from original DoA

1.4.1 Description of work related to deliverable as given in DoA

The Project handbook contains operational procedures and processes for the project regarding information sharing, meetings, quality assurance, risk management and ethics (the informed consent procedures that will be implemented for the participation of humans). It also contains updates of the project progress so far.

After being submitted in M4, the Project handbook remains a dynamic document. E.g, if the data management plan needs to be updated, that results in a new version of the Project handbook.

1.4.2 Time deviations from original DoA

The submission of the deliverable was postponed in order to include an update and summaries of the first deliverables. There is total delay of 70 days.

1.4.3 Content deviations from original DoA

There are no deviations from the DoA; the content of this deliverable is in line with the plan. Additionally, the summaries and updates of the first deliverables was included.

2 Management structure

Both the Grant Agreement and the Consortium Agreement specify a number of bodies for the management of the project. Though the two Agreements, being legal documents that can be found on SharePoint, take precedence over this handbook, the following sections specify the operational view of these bodies.

The project is divided into a set of WPs which complement each other and support the progress towards the objectives of the project. Each WP complies with the objectives and schedule of the project and delivers results in accordance to what has been agreed and within the allocated resources. The research and development activities will be carried out in the WPs where domain, partnership and resource allocation have been well defined.

The monitoring, control and steering of the project are executed by the General Assembly (GA) and the Core Group (CG) coordinated by the Project Coordinator (PC).

2.1 Project Coordinator (PC)

The Coordinator is Zissis Samaras (LAT/AUTh). Support is provided by two Project Managers: Dimitrios Kontses (LAT/AUTh) and Savas Geivanidis (LAT/AUTh).

Tasks:

- Development and management of the project plans, reviewing the plans regularly to ensure tasks and milestones are being achieved in a timely manner
- Fulfilment of the obligations of the Coordinator under the Grant Agreement with the European Commission
- Interaction with the European Community and third parties about the project, including the submission of deliverables to the European Community.
- Representation of the project towards the European Community and other third parties but shall not be entitled to act or to make legally binding declarations on behalf of any other partners.
- Receiving, compiling and distributing to the partners, documents, reports, statements of expenditure, minutes of meetings of the GA and the CG.

2.2 Work package leaders

The work package (WP) is the building block of the project. The WP leader:

- Monitors the work and the progress of the Work Package
- Supervises and provides day to day management of the activities of the respective partners
- Performs active planning and progress monitoring of the Work Packages
- Executes her/his own control over internal issues
- Ensures the information exchange about the Tasks with the other partners participating in the WP.

Current WP leaders are shown in Table 1.

Table 1: Current WP leaders

WP	WP Name	Current WP Leader

WP1	Consortium and project management	Georgia Parpori (LAT/AUTh)
WP2	Inception, concept final revision and monitoring of project targets	Dimitrios Kontses (LAT/AUTh)
WP3	Market analysis and assessment of tampering systems	Delahaye, Ann (TNO)
WP4	Security mechanisms for hardened and tamper proof vehicular systems	Obaid Ur-Rehman (FEV)
WP5	Development and demonstration of DIAS advanced diagnostic solution	Andreas Hastall (BOSCH)
WP6	Synthesis and evaluation, dissemination and exploitation of results	Savas Geivanidis (LAT/AUTh)
WP7	Ethics requirements	Savas Geivanidis (LAT/AUTh)

2.3 Core Group (CG)

Tasks:

- Supervises the progress of the project from its start-up phase to its completion, guaranteeing its continuity and consistency and allocating the resources adequately.
- Assuring cooperation and integration between the WPs as defined in the workplan
- Is in charge of making decisions or proposals for decisions to be taken by the GA.
- Handles any conflict resolution within the project which could not be handled at a lower level.
- When necessary, e.g. due to a technological breakthrough, adjusts the content and direction of research in the project.
- Performing risk analysis and preparing contingency plan

Members:

- All WP Leaders (Table 1)
- Level of representative is senior research manager.

Chairperson:

The Coordinator of the project chairs the meetings of the CG.

2.4 General Assembly (GA)

Tasks:

- Reviews and monitors the progress and the activities of the project.
- Identifies appropriate actions for the successful performance of the project reviewing the plans for the remaining phases.
- Takes decisions of major and strategic relevance regarding the project and does not interfere with internal WP issues unless these disturb the project itself or its other WPs.

Members:

- One representative per each partner of the project. The current GA-members are listed in Table 2. The members of the GA are referred to as ‘partner manager’.
- Level of representative is senior research manager.

Chairperson:

The Coordinator of the project chairs the meetings of the GA.

Table 2: Current partner managers

Nr	Partner	Partner manager
1	ARISTOTELIO PANEPISTIMIO THESSALONIKIS	Zissis Samaras
2	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	Ann Delahaye
3	ROBERT BOSCH GMBH	Ian Faye
4	ROBERT BOSCH AG SWITZERLAND	Dominic Woerner
5	FEV EUROPE GMBH	Christof Schernus
6	UNIVERSITATEA DE MEDICINA, FARMACIE, STIINTE SI TEHNOLOGIE "GEORGE EMIL PALADE" DIN TARGU MURES (UMFST)	Piroska Haller
7	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	Konstantinos Votis
8	FORD OTOMOTIV SANAYI ANONIM SIRKETI	Dincer Ozcan
9	ICCT - INTERNATIONAL COUNCIL ON CLEAN TRANSPORTATION EUROPE GGMBH	Felipe Rodriguez
10	JRC -JOINT RESEARCH CENTREEUROPEAN COMMISSION	Georgios Fontaras
11	VRIJE UNIVERSITEIT BRUSSEL	Nils Hooftman

2.5 Communication Board (CB)

A formal internal Communication and Dissemination Plan is currently generated in the DIAS project (part of Deliverable 6.1), and a Communications Board (CB) will be established at the next general assembly to be charged with overseeing and implementing this communication and dissemination strategy. The CB will be comprised of members from LAT/AUTh.

2.6 Advisory Board (AB)

The Advisory Board consists of a limited number of external experts that will be selected on the basis of their profound and long-lasting expertise in the field of research. The AB members will be invited to general progress meetings of the project or technical WP meetings where they can advise the consortium and help DIAS to address and overcome technical issues that may arise.

The advisory board will be established at the next general assembly meeting. Members of the Advisory boards are selected in agreement with the PO.

3 Quality procedures and Code of Conduct

3.1 Internal communication structures & procedures

The Consortium Agreement specifies a number of rules for the governance of the project. Though the Consortium Agreement takes precedence over this handbook, the following describes the operational view of project meetings.

3.1.1 GA Meetings

Every 6 months a GA meeting will be scheduled. If important decisions need to be taken at GA level, then an ad-hoc meeting can be scheduled.

The agenda will be distributed at least two weeks before the meeting. All partner managers can enlist agenda items for the GA meeting.

No minutes are taken at the GA meetings, but decisions and actions of the GA are listed. These decisions and actions are shared with the WP leaders via the consortium manager in the first CG meeting after the GA meeting.

3.1.2 CG meetings

Every two weeks the CG has a conference call (additional member e.g. task leaders can also participate). The main purpose of these meetings is the alignment of work between the WPs.

The agenda will be distributed approximately one week before the meeting.

The decisions and action points of the CG meetings are communicated to all CG and GA members by the consortium management via e-mail. For that purpose, the agenda of the CG meeting is extended, within two working days after the CG meeting, with the actual participants list, the decisions and action points. The extended agenda is shared on SharePoint. This allows GA members to react, e.g. if decisions are taken in an CG meeting and a GA member considers that decision to require GA endorsement.

3.1.3 WP and task meetings

For meetings within the WP, the WP leaders have full freedom to arrange them as they wish. The only constraint will be the travel budget of the partners.

If a partner is not participating fully in the WP or task, and there is a risk of that partner becoming a ‘defaulting partner’, as defined in the Consortium Agreement, then the following steps will be taken.

- The manager of the task/WP will have a private discussion with the partner. The result will be recorded in an e-mail, sent in Cc to the consortium manager. In the unlikely case the WP leading partner is not fully participating, any partner in the WP can signal this to the consortium manager, initiating the next step immediately.
- If this fails to produce the desired behaviour or if a WP leader is not participating fully in the WP, the consortium manager will have a private discussion with the partner. The result will be recorded in an e-mail, sent in Cc to the General Assembly.
- If this fails to produce the desired behaviour, the GA starts the ‘defaulting partner procedure’ as defined in the Consortium Agreement.

3.2 External communication structures & procedures

The following key groups are identified in the external communication. In all other cases the CG will propose how to proceed. Wherever there is a risk of confidential information of any partner being disclosed, the 'GA check', as described in section 3.3.1.3, has to be applied.

For all material used in the external communication, the quality assurance/review procedures, as described in 3.3.2, apply.

3.2.1 Advisory boards

All communication with the AB members is coordinated by the scientific lead.

Support will be provided by those project members who already have a personal relation with the AB members and the consortium management

All communication with the AB is coordinated by the WP6 leader.

Support will be provided by those project members who already have a personal relation with the AB members.

3.2.2 EC

All communication with the European Commission (EC), and in particular with the project officer (PO), will be coordinated by the consortium management as defined in Table 3. Where needed the Scientific lead will support the consortium management in this.

Table 3: Consortium Management

Role	**Person**
Consortium manager	Zissis Samaras (LAT/AUTh)
Consortium management Support	Savas Geivanidis (LAT/AUTh), Dimitrios Kontses (LAT/AUTh), Pavlos Fragkiadoulakis (LAT/AUTh)

3.2.3 Related projects

Exchange of information with related projects will be coordinated by the WP6 manager. All partner managers will be informed prior to any exchange and, if necessary, separate NDAs will be signed. Further support can be provided by partners already having personal relations with project members of the related project.

Project members should be aware of the fact that exchange of information with related projects might require an NDA prior to the information exchange.

3.3 Quality of (non-)deliverables and peer review

Reviews are the key elements in the quality assurance of a project like DIAS. For the review process there is a distinction between review of deliverables and the review of other material.

3.3.1 Deliverables

For deliverables good planning is possible, since a global description of the content, the submission date and the partners working on it are set out in the DoA. The review will be done in three stages:

- Structure or scope review
- Content review
- GA check

Two independent reviewers are appointed by the CG for each deliverable, and in principle both perform the structure/scope and the content review. Reviewers are considered independent when they are not authors of the deliverable. Of course, others are free to review too, but the appointed reviewers take on the quality assurance responsibility for the deliverable.

3.3.1.1 Structure or scope review

The input for the structure review is the structure description of the deliverable. The structure description consists of at least two levels in the table of contents, chapters and sections. At section level there is

- a 5-line description of the content,
- the responsible partner/person for generating the content,
- and the expected number of pages as indicator for the level of detail.

The structure review starts as soon as the structure description is available, but not later than 8 weeks before the submission date of the deliverable. Reviewer comments are to be submitted to the deliverable editor 7 weeks before the submission date.

3.3.1.2 Content review

The input to the content review is the full deliverable text; only supporting parts – references, list of abbreviations and annexes – might still need completion.

The content review starts at the latest 3 weeks before the submission date. Review comments are submitted to the deliverable editor 2 weeks before the submission date.

In general, the content review contains four main attention areas.

- DoA coverage
  - Is the scope and the content of the deliverable consistent with the intention of the deliverable as stated in the DoA?
  - In case of deviations, are they fully and plausibly motivated?
  - Are the relations to other DIAS work/deliverables clear? Deliverables are rarely produced in splendid isolation, so … a deliverable provides input to other work, or brings other work together, or …
- Target audience
  - Is the target audience clear?
  - In case of multiple target groups, is it clear what parts of the deliverable are intended for each audience?
  - Are the management summary, introduction and conclusions/recommendations at the level, and using the language, of the target audience?
    Note: The detailed content might be too detailed for all target groups, but not the sections mentioned above.

- Are the conclusions fully backed by the preceding material (no “jumping to conclusions”) and are recommendations actionable?

- Language and structure
  - Is the language used proper international English?
    Signal use of national variants – Dunglish, Gerlish, Itlish, … – and sociolects – legalish, techlish, ...
    In case of doubt, consult a native English speaker.
  - Is the text well-structured, e.g. using lists and tables where appropriate? Pages with a grey rectangle of text are suspicious.
  - Do chapters have a local introduction/purpose and local conclusions/recommendations?
  - Are illustrations and diagrams used to support the text where appropriate? If taken from external sources, is the attribution correct/complete?
  - Are references to literature included – sufficient but not overdone?
- Technical content
  - < For the editor/WP leader to guide the review process>

3.3.1.3 GA check

The GA members receive the deliverable one week before the submission date. They check that the deliverable does not disclose commercially sensitive information of their organisation. If the deliverable contains material from non-partners that is made available via their organisation, the GA member checks that the deliverable respects the confidentiality agreements made by their organisation with the non-partners.

Note: the GA check is not a classical review. It is an ‘emergency break’ if confidential material is about to be disclosed and this was not noted by authors and reviewers.

Both submissions to reviewers are Cc-d by the deliverable editors to the consortium manager. The submission to the GA for the GA check is done by the consortium management. Deliverables are uploaded to the Participant Portal – Continuous Reporting and submitted by the consortium management.

The timeline for deliverables is depicted in Figure 1.

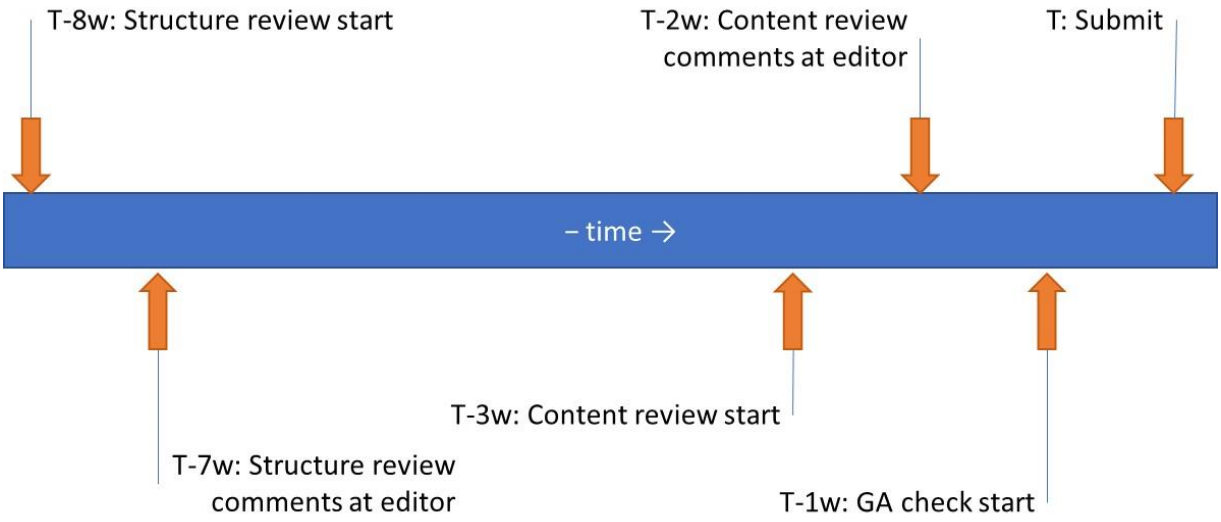

Figure 1: Timeline deliverable review

3.3.2 Non-deliverables

For non-deliverables, such as publications and dissemination material, the procedure for deliverables will be used where applicable and with a timeline that fits the material.

In all cases the CG is required to be informed via the WP leader about the intention to publish DIAS material as early as possible, with a minimum of 4 weeks. The CG will decide on the review procedure for that case. This is enabled by WP leaders signalling planned academic publications or conference contributions to the Scientific lead and signalling non-academic work to the WP6 lead.

Since there are many types of material, this handbook cannot provide details for all cases. We distinguish the following broad categories of material.

- Dissemination material (flyer, website, leaflets, popular science publications, …)
  Default reviewer is the consortium manager, supported by one or more partner managers.
- Scientific publication or conference presentation
  Default reviewer is the scientific lead, supported by one or more partner managers.

3.4 Risk management

In the GA the results of an initial risk assessment are listed. This is considered the initial risk register.

When a partner or WP leader identifies

- a new issue or potential risk,
- an issue becoming a risk,
- a substantial rise of a risk, either because the chance of occurrence gets higher or the expected impact becomes bigger,

then this should be communicated with the consortium management as soon as possible. At the latest at the next CG this issue and potential measures will be discussed in an attempt to avoid an issue becoming a risk. At the next CG it will be checked if the issue containing measures were/are sufficient, or if the issue

becomes a real risk. In the latter case it will be added to the risk register, with the associated mitigating actions.

Periodically, approximately once every 6 months, the risk register will be reviewed in the CG. On this occasion, risks that cannot occur any longer, or became very small, will be removed.

3.5 Project templates

The DIAS project intends to use a consistent 'project style'. This is implemented by providing templates for the deliverables, the presentations and dissemination materials. More project style templates can be produced by WP6 when needed.

All available project style templates can be found on the DIAS SharePoint (available only for members).

For the publications created separately by the partners, the following acknowledgment is required by the EC: *This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.*

For abstracts, presentations, summaries etc. that will be published together with the publications, the DIAS and EU logos should be included if possible.

3.6 Technical coordination

The Project Coordinator will carry out technical coordination activities such as planning of technical work, deliverables, assessment of technical progress, consolidation and review of deliverables and technical (progress) reports.

The research work has been divided in logical parts for which work package leaders and task leaders have been assigned to co-ordinate the activities within that specific work package and tasks. At the start of each individual work package and task, the involved partners will precisely define the content of each deliverable including its assessment criteria. What questions and issues need to be answered/solved, how this will be done, when this will be done and by whom will this be done.

For each task group, the task leader, in conjunction with the work package leader, can specify intermediate deliverables in order to facilitate progress monitoring (e.g. quarterly). Task groups composed of engineers/researchers performing the individual tasks will hold meetings whenever relevant. The task leaders will chair these task meetings. Each task leader will report to their work package leader on a regular basis.

3.7 Progress monitoring

Communication among partners will be realised via various channels: email, website, call conference, periodic meetings. Every three months each WP leader is requested to provide a short management report mentioning the major achievements/progress and problems encountered (critical or not critical). The progress reports will be discussed in the CG meetings. During periodic GA meetings, each partner will inform the GA and PC about their progress and plans for upcoming period.

4 Tools and communication infrastructure

4.1 Document sharing

One key element in a research project like DIAS is collecting/sharing/analysing information and the collaborative production of reports on the results of the analysis.

For both purposes a SharePoint environment has been created with URL: https://latengauthgr.sharepoint.com/sites/dias-project

Within this SharePoint environment directories are available for each WP, along with all submitted deliverables. Furthermore, lists are maintained for project members and external contact persons.

Partner managers should announce a new project member to DIAS SharePoint manager. Name, e-mail address and a mobile telephone number (able to receive a text message (SMS) for the access) are sufficient for creation of the SharePoint access. All project members have to provide their contact details in the project member list.

If a project member leaves the project, this should also be reported to DIAS SharePoint manager.

4.2 E-mail and telephone

Day to day information exchange will be based on e-mail and telephone.

Basic rule for exchange of information via e-mail: never include a document larger than 50 kB in an e-mail. Provide in the e-mail a link to the document, stored on SharePoint instead.

The available e-mail distribution lists are listed in Table 4. Mailing lists are also available as Outlook items at the SharePoint site.

The files contain current information and will be updated accordingly after any change (Table 4):

Table 4 Mailing lists as downloadable Outlook items

Mailing list	**Contains**
DIAS_ALL.msg	All project employees working in WPs below
DIAS_CG.msg	All members of core group + coordination team
DIAS_GA.msg	All members of general assembly + coordination team
DIAS_MC.msg	Main contact persons
DIAS_WP1.msg	All project employees working in WP1
DIAS_WP2.msg	All project employees working in WP2
DIAS_WP3.msg	All project employees working in WP3
DIAS_WP4.msg	All project employees working in WP4
DIAS_WP5.msg	All project employees working in WP5
DIAS_WP6.msg	All project employees working in WP6

DIAS_WP7.msg	All project employees working in WP7

Partner managers should announce a new project member to the Consortium management Support and indicate the e-mail lists the new project member should be in. Project members leaving the project will be deleted from the e-mail lists.

4.3 Online meetings

Online meetings, such as the CG meetings, will use 'Skype for Business'. This tool supports screen sharing, making it possible to discuss lists of action points and decisions, presentations, etc.

4.4 Progress reports

One of the risks of working in a consortium is that one of the partners spends a lot of effort without reaching a substantial result. To avoid this happening without the WP leader and the consortium manager being aware, the effort of each partner shall be reported every quarter.

The tools used for this monitoring are the *Financial internal report (months x-x)* and the *PM internal report (months x-x),* two Excel based tools where the partner reports the costs and the person months spent in the recently closed quarter for each WP. Figure 2 shows a part of the PM internal report Excel sheet for the first 6 months.

PM - CONSUMED							
	Period 1		Period 2		Period 3		Total
Work Package	Month 1-6	Month 7 - 12	Month 13 - 18	Month 19 - 24	Month 25 - 30	Month 31 - 36	
WP1 - Consortium and project management							0.00
WP2 - Inception. concept final revision and monitoring of project targets							0.00
WP3 - Market analysis and assessment of tampering systems							0.00
WP4 - Security mechanisms for hardened and tamper proof vehicular systems							0.00
WP5 - Development and demonstration of DIAS advanced diagnostic solution							0.00
WP6 - Synthesis and evaluation, dissemination and exploitation of results							0.00
WP7 - Ethics requirements							0.00
Total	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Figure 2: PM internal report months 1-6 fragment

The consortium management will consolidate all partner inputs. In the CG it is checked if the effort as reported is balanced with outputs of each partner.

QPR timeline:

- The partner managers receive a request for reporting on the first week of the month after closing a quarter.

- The partner manager reports the effort at the latest on the 15th of the month after closing a quarter.
- The consolidated reports are available at the latest on the 22nd of the month after closing a quarter and will be on the agenda of the first CG after the 22nd.

5 Ethical guidelines

Ethics is an integral part of responsible research, from the conceptual phase to the publication of research results. The DIAS consortium is clearly committed to show appreciation of potential ethical issues that may arise during the course of the project and has as such defined a set of procedures on how to deal with ethics in a responsible way.

The main aspects the project is dealing with in regard to ethics are the protection of individuals and the environment. For the individuals, key elements are the protection of identity, privacy, obtaining informed consent and communicating benefits and risks to the involved target groups.

The studies performed in DIAS may include data collection from individuals and organisations remotely as well as on site. In order to achieve the goals defined within the research tasks of the work programme the consortium may collect personal data from study participants. Such data may include basic demographic data, responses to questionnaires or interaction data with technologies.

5.1 Health and safety

Some of the tasks will require laboratory or garage work. This work will be performed by certified engineers trained to follow the national health had safety regulations. No work is foreseen that requires additional health and/or safety measures.

5.2 Data protection and privacy

First of all, it should be noted that the participation in an activity aimed at evaluating tampering of vehicles in relation to use of vehicles in real world conditions (i.e. recording of engine and vehicle related parameters) and effectiveness of current and DIAS systems to reduce tampering hardly generates any threat to the privacy of the participating volunteers. However, one can imagine exceptional cases with a small risk, and therefore DIAS will take appropriate measures. Since such activities are of a different nature, the appropriate measures will be defined during the project on a case by case basis.

During any data collection process data protection issues involved with handling of personal data will be addressed by the following strategies.

Volunteers to be enrolled will be exhaustively informed, so that they are able to autonomously decide whether they give their consent to participate or not. The purposes of the research, the procedures as well as the handling of their data (protection, storage) will be explained. For online interviews these explanations will be part of the initial briefing of interviewees, for face-to-face interventions informed consent (see below) shall be agreed and signed by both, the study participants as well as the respective research partner.

The data exploitation will be in line with the GDPR and the respective national data protection acts. Since data privacy is only under threat when data are traced back to individuals – they may become identifiable and the data may be abused – we will anonymise all data. Furthermore, where identification data is not required by the research task at hand, those data shall not be recorded, following the privacy by design principle. Alternatively, the partner, might act as data gathering organisation and provide only the anonymised data to DIAS.

The data gathered through questionnaires, interviews, observational studies at the workplace, focus groups, workshops and other possible data gathering methods during this research will be anonymised and therefore the data cannot be traced back to the individual. Data will be stored only in anonymous forms so the identities of the participants will only be known by the research partners involved. If raw data like interview protocols and audio files need to be shared among the consortium partners, this will only be done after the confidentiality agreement (See Annex A – Confidentiality Agreement) has been signed. Reports based on interviews, focus group and other data gathering methods will be based on aggregated information and comprise anonymous quotations respectively.

The strategies above will be elaborated per activity and require the approval of the Data Protection Officer (DPO) of:

- the data collecting organisation, either a consortium partner and/or an external partner;
- LAT if the data collecting organisation has no DPO;

The DPOs of the partners, including their contact data, are listed in Table 5.

Table 5: Data Protection Officers contact data

Nr	Partner/Organization	DPO	Email	Phone
1	ARISTOTELIO PANEPISTIMIO THESSALONIKIS	Angeliki Agorogianni	*Upon request*	*Upon request*
2	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	Remy van den Boom	*Upon request*	*Upon request*
3	ROBERT BOSCH GMBH	Rainer Saxarra	*Upon request*	*Upon request*
4	ROBERT BOSCH AG SWITZERLAND	Veronika Deimel	*Upon request*	*Upon request*
5	FEV EUROPE GMBH		*Upon request*	*Upon request*
6	UNIVERSITATEA DE MEDICINA, FARMACIE, STIINTE SI TEHNOLOGIE "GEORGE EMIL PALADE" DIN TARGU MURES (UMFST)	Demian Dorel Augustin	*Upon request*	*Upon request*
7	ETHNIKO KENTRO EREVNAS KAI	Ioannis Chalinidis	*Upon request*	*Upon request*

	TECHNOLOGIKIS ANAPTYXIS			
8	FORD OTOMOTIV SANAYI ANONIM SIRKETI	Does not need one based on the regulatory definitions		
9	ICCT - INTERNATIONAL COUNCIL ON CLEAN TRANSPORTATION EUROPE GGMBH	Does not need one based on the regulatory definitions		
10	JRC -JOINT RESEARCH CENTREEUROPEAN COMMISSION	Spyros Konstantinidis	*Upon request*	*Upon request*
11	VRIJE UNIVERSITEIT BRUSSEL	Wessel Damen	*Upon request*	*Upon request*

6 Open access and open research data

The DIAS project firmly believes in openness to be a major factor for innovation. There are many examples of how open innovation and open source are successful models, especially in domains where many different stakeholders are required to bring about effective change. Openness has many facets. The most important ones for the DIAS consortium are:

- Open project collaboration. All partners are committed to developing (working for) relationships with external partners for mutual benefit. Making contacts with similar projects and establishing collaboration with potential stakeholders is considered beneficial for all.
- Open source technology. Tools to produce normalized engine maps are intended to be made available as open source. However, considering the liability associated with tools for in-car use, the consortium members consider these as not suited for open source.
- Open access to scientific results. From a scientific perspective, the consortium clearly favours open access to its scientific output, which is supported by several project members' internal policies of supporting open access in general.
- Open access to research data. The general policy of the DIAS project is to apply "open by default" to its research data, with exceptions being made based on privacy, competitiveness, and ethical rules on anonymity are thus highly relevant and need to be agreed with each of the partners and stakeholders.
- In general, any data or information collected or produced during the project the sharing of which will facilitate any illegal actions including but not limited to tampering will not be made publicly available.

The open access strategy will be detailed in the following sections.

6.1 Open access strategy for publications

In line with the EC policy initiative on open access , which refers to the practice of granting free online access to research articles, the project is committed to follow a publication strategy considering a mix of both 'Green open access' (immediate or delayed open access that is provided through self-archiving) and 'Gold open access' (immediate open access that is provided by a publisher) as far as possible.

All deliverables (reports, software, data, media, other) labelled as "public" will be made accessible via the DIAS website (www.dias-project.com). The publications stemming from the project work will also be made available on the DIAS website.

Where appropriate, the results will also be published via ResearchGate (https://www.researchgate.net/), preferably via the accounts of scientists that already have a track record in this domain (i.e. no DIAS account).

All outcomes of the project labelled as "public" will be distributed under specific free/open license, where the authors retain the authors' rights but the users can redistribute the content freely.

6.2 Data management plan (DMP)

A data management plan (DMP) describing the data management strategies in more detail is currently developing by the DIAS consortium and will be available within the first eight months of the project (see Deliverable D6.2). Table 6 gives an outline of the DMP to be developed. Updates of the DMP are planned

around the middle of the project, by which point the first sets of city-specific data will have been generated, as well as toward the end of the project.

Table 6: General outline of data management plan

Action	*Target*
Project, experiment, and data description	**What's the purpose of the research?**
	What is the data? How and in what format will the data be collected? Is it numerical data, image data, text sequences, or modelling data?
	How much data will be generated for this research?
	How long will the data be collected and how often will it change?
	Are you using data that someone else produced? If so, where is it from?
	Who is responsible for managing the data? Who will ensure that the data management plan is carried out?
Documentation, organization, and storage	What documentation will you be creating in order to make the data understandable by other researchers?
	What file formats will be used? Do these formats conform to an open standard and/or are they proprietary?
	Are you using a file format that is standard to your field? If not, how will you document the alternative you are using?
	What are your local storage and backup procedures? Will this data require secure storage?
	What directory and file naming convention will be used?
	What tools or software are required to read or view the data?
Access, sharing, and re-use	Who has the right to manage this data?
	What data will be shared, when, and how?
	Does sharing the data raise privacy, ethical, or confidentiality concerns?
	Who holds intellectual property rights for the data and other information created by the project? Will any copyrighted or licensed material be used? Do you have permission to use/disseminate this material?
	Are there any patent- or technology-licensing-related restrictions on data sharing associated with this grant?
	Will this research be published in a journal that requires the underlying data to accompany articles?
Archiving	How will the data be archived for preservation and long-term access?
	How will data be prepared for preservation or data sharing
	Are software or tools needed to use the data? Will these be archived?
	How long should the data be retained?

7 Progress and preliminary achievements

7.1 Kick-off meeting

DIAS first official meeting was held on October 23-24, 2019 (Thessaloniki).

a) Audience

This event was attended by project's Officer and representatives from each institution involved in the project. The encounter was a unique occasion for them to meet each other at the beginning of the project.

Participants of the kick-off meeting were:

Affiliation	Name
LAT	Savas Geivanidis
LAT	Zisis Samaras
LAT	Dimitrios Kontses
LAT	Athanasios Dimaratos
LAT	Georgia Parpori
TNO	Ann Delahaye
TNO	Robin Vermeulen
TNO	Frank Kupper
FEV	Christof Schernus
FEV	Obaid Ur-Rehman
Bosch	Andreas Hastall
Bosch	Ian Faye
Bosch	Markus Willimowski
Bosch IoT	Dominic Woerner
CERTH	Anastasios Drosou
CERTH	Sofia Terzi
CERTH	Anastasia Theodouli
CERTH	Ioannis Xygonakis
CERTH	Kostantinos Moschou
Ford	Emrah Kınav
UMFST	Bela Genge
UMFST	Piroska Haller
VUB	Nils Hooftman
JRC	Georgios Fontaras
JRC	Fabrizio Forloni
ICCT	Felipe Rodriguez
INEA/EC	Marina Kousoulidou

b) Contents

The DIAS work plan was discussed and, as reported in this document, no major changes were brought.

Each leader gave a short overview of its work package, outlining

i) Objectives, tasks, deliverables and resources
ii) Timing and deliverables
iii) Interrelation between WPs
iv) other open points for discussions

This considerably improved working relations among partners

It was decided that:

- The General Assembly will meet every six months per year (March and September timeframe)
- The Core Group will hold a bi-weekly teleconference (via Skype for Business) to organise the technical work
- A specific project website and intranet has been launched and used having two separate domains: a public www.dias-project.com and a restricted domain (via login in Microsoft SharePoint)
- Next GA meeting will be held on March 11th-12th, 2020 (The meeting was postponed by the Co-ordinator for the April 8th-9th, 2020) Detailed minutes of the Kick-off meeting, of the thematic workshops and PowerPoint presentations for each WP have been circulated among the consortium and will be available in the restricted section of the DIAS website (SharePoint).

7.2 Work Plan

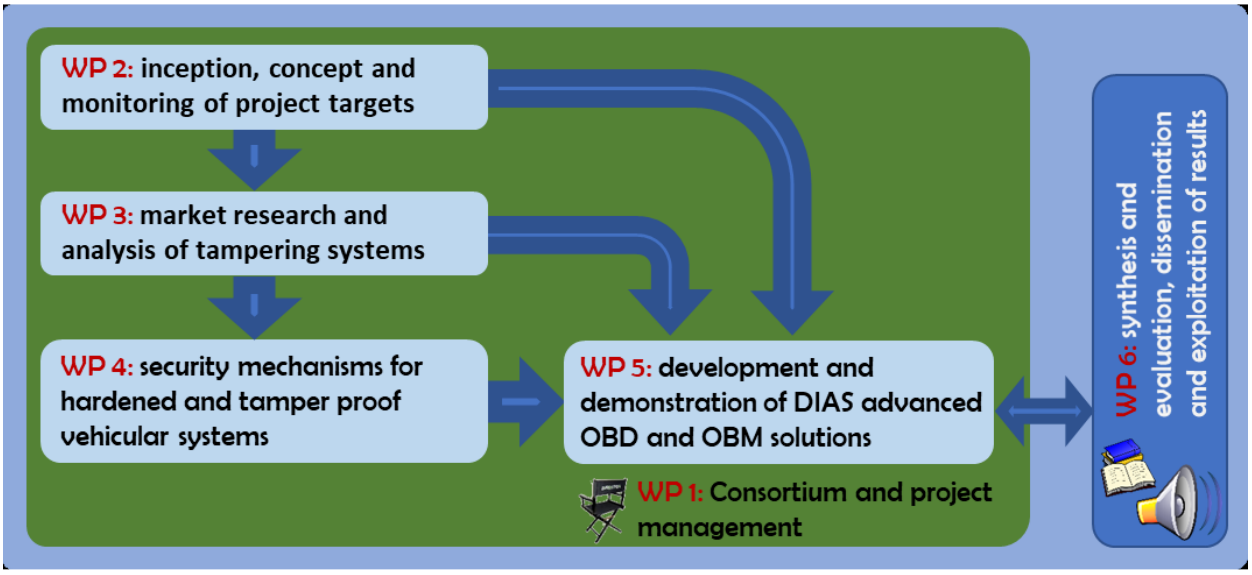

Figure 3: Project work package structure

7.3 WP1

a) Review of WP objectives

The objectives of WP1 have been already described in the previous sections.

b) Progress so far

The kick-off meeting and several teleconferences have been organized to coordinate the DIAS activities.

7.4 WP2

a) Review of WP objectives

- Review for tampering practices across the EU and globally
- Description of project targets
- Use case definition
- Successful achievement of project targets in a technology neutral way allowing tamper-proof systems at the most advanced approach proposed
- Technology neutral and universally applicable industry-wide methods and monitoring system architectures.

b) Progress so far

Deliverable D2.1 has been completed by WP2 members. Executive summary:

The state-of-the-art vehicle environmental protection systems (EPS) can successfully retain the emissions at low levels. However, tampering attempts with these systems are evidently increasing and this can significantly reduce their effectiveness. The reasons and motivations are related to the security of current On-Board Diagnostic (OBD) systems which need to be improved and the cost-benefit that can result for the vehicle owners.

This report documents an overview of current and (near-term) future tampering techniques. The methodology followed to achieve the target of this work included a literature review and extensive communications with tamperers. Following the introduction in chapter 1 regarding the background of DIAS and the purpose of this document, the study is structured around the chapters below:

- Chapter 2: Methodology
- Chapter 3: Tamperers
- Chapter 4: Current tampering practices
- Chapter 5: Future issues

The study concludes with the summary in chapter 6.

Chapter 2 discusses the methodology and sources which were used in the current deliverable.

Chapter 3 categories the tamperers into 4 main levels:

- Level 1: Inexperienced individuals
- Level 2: Moderately experienced individuals
- Level 3: Highly experienced mechanic specialists
- Level 4: Highly experienced programmer specialists

Levels 1 and 2 have limited capabilities and the target-area is mainly tampering with older vehicles and simpler systems compared to the specialists. Levels 3 and 4 are usually in close cooperation with each other and work in tampering workshops.

Chapter 4 focuses on the current tampering practises (until early Euro 6/VI vehicles). The analysis shows that emulators and ECU flashing are the prevailing general practises for all EPS. Emulators are considered

low-cost but questionable solutions with regard to reliability and are mainly applied in old vehicles from inexperienced individuals whereas specialists prefer the ECU flashing techniques as the only reliable solution. The options for gaining access to the ECU are also described and a few typical examples are presented. The next part of this chapter provides details for each of the main exhaust aftertreatment components that are tampered: SCR, DPF, EGR and TWC. Finally, the effect and the techniques related to the vehicle tuning are presented in the last part of this chapter.

Chapter 5 contains the future issues that will affect tampering practices. More advanced vehicle security systems (e.g. Secure CAN) will require new approaches for access to the ECU and smarter emulators. The available information though is limited, and continuous updates will be provided in the future when tamperers will be confronted with the new advanced vehicle systems.

7.5 WP3

a) Review of WP objectives

Available in the website

a) **Progress so far**

Deliverable D3.1 has been completed by WP3 members. Executive summary:

Pollutant emissions of road vehicles have reduced significantly thanks to the development and application of effective and often complex emissions control systems. Tampering of these systems leads to elevated emissions levels 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.

For task 3.1 of DIAS, a market assessment was conducted 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. The exercise has led to a proposal for a test matrix of vehicle – tampering combinations that poses the largest environmental risk and which should be tested in the next phase of the project to determine the current vulnerabilities and exploits of vehicles that need to be addressed by the DIAS concept. The following conclusions can be drawn:

- There is a substantial market where tampering is offered for both light- and heavy-duty vehicles and non-road mobile machinery. However, not much quantitative information is available which indicates the magnitude of the problem, i.e. the number of vehicles that are tampered in the EU.

- An important source that does indicate tampering in the EU are roadside inspections for trucks where significant tampering rates were found for previous generations of heavy-duty vehicles for which an advanced emissions control system is required (Euro IV and V). The inspections are however often selective, targeting specific vehicles based on experience and assumptions, most likely resulting in biased data. The magnitude of the problem is largely unknown for Euro VI and the light-duty and non-road mobile machinery segments.

- The motive mentioned motive for tampering is to avoid costs for repair of malfunctions of the emissions control systems of diesel engines. Other motives mentioned are: costs for consumables, costs for downtime, performance tuning and exhaust sound level.

- Emissions control systems with higher rates of malfunctions and related costs for repair may therefore pose the largest environmental risk: 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.

Two main types of tampering were found for vehicles of the latest generation, backed up by findings of consortium partner LAT:

1. Emulators
2. ECU (Engine Control Unit) reprogramming (also called ECU flashing, ECU remapping)

This tampering is either offered as a service in workshops or as product with instructions for installation offered on the internet in web shops, online shopping areas, forums and social media. OBD (On-Board Diagnostics) diagnostic trouble codes (DTC) may arise when tampering leads to errors detected by the current OBD. Diagnostic Trouble Code deletion tools are offered to support the tampering, i.e. to by-pass periodic inspection and to avoid power inducement of the engine forcing an owner to repair the malfunction.

Other types of tampering exist which should also be assessed regarding the possible risk:

- Tampering and emulation of temperature sensors so that temperatures outside the window of normal operation are generated to fool and shutdown the emission control system.
- A miniature catalyst installed in front of the lambda sensor that provides a correct air fuel mixture to the sensor, while in fact the mixture is not correct, such that no error is generated.

The market assessment has led to a test matrix in which the vehicle-tampering combinations that most likely pose the largest environmental risk are defined. The test matrix contains light- and heavy-duty vehicles and non-road mobile machinery with diesel engines, the two main types of tampering devices and services, the OBD DTC delete tool and temperature sensors tampering.

A list with tampering devices and services found to date was compiled. This list will be further expanded when new or other tampering is found in the course of the project. The market assessment will be continued in order to better define the magnitude of the problem and scan the market for other or new types of tampering.

Other relevant observations made during the tampering market analysis and assessment are:

- There is an increased intensity of roadside inspections with prosecution and sanctioning by several EU Member States, mainly for heavy-duty vehicles.
- There is an increased stringency of requirements for OBD and control of NOx measures (EU) towards current EU requirements (Euro 6dtemp, VI step-D, stage V).
- There are plans by some EU member states for checking the DPF at periodic inspection.

These measures may already lead to a less attractive ‘environment’ for tampering.

7.6 WP4

a) Review of WP objectives

Available in the website

a) **Progress so far**

Deliverable D4.1 is under internal review process

7.7 WP5

a) Review of WP objectives

Available in the website

a) **Progress so far:** None to reportWP6

7.8 WP6

a) Review of WP objectives

- Visible dissemination of the project's results and maximize its impact to relevant stakeholders and audience at the EU-level.
- Interactive ongoing dialogue with key stakeholders such that DIAS follows up on their interests and background to effectively influence policy and practice.
- Establishment of links with relevant projects in EU, USA and Japan.
- Exploitation plan defining best practices, protocols and technologies which can contribute to current regulatory measures.
- Guidelines and recommendations for future legislation

a) Progress so far

In order to share the goals and results of the Project as well as to get a widespread attention among different users in Europe and elsewhere the following logo has been chosen

DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Figure 4: DIAS logo

Project's website has been created. The website is user friendly and has two separate domains: a public www.dias-project.com and a restricted domain (via login). It includes the basic information about the

project, description of the cases, the most relevant documents accounting for the cases (e.g. reports, publications, etc)), analyses, guidance and recommendations.

Also, a Twitter account (DIAS project, @DIAS_project) has been created to easily communicate the news, events, meeting etc. of DIAS project.

7.9 WP7

a) Review of WP objectives

The objective is to ensure compliance with the 'ethics requirements'.

a) Progress so far

Deliverable D7.1: NEC - Requirement No. 1

8 References

AECC. (2018, 01). NEWSLETTER, International Regulatory Developments. Retrieved from https://www.aecc.eu/wp-content/uploads/2018/02/AECC-Newsletter-January-2018.pdf

Pöhler et al. (2017). Real Driving NOx Emissions of European Trucks and Detection of Manipulated Emission Systems. *Geophysical Research Abstracts*, 19.

Spreen, J. S., Kadijk, G., & Van der Mark, P. (2016). *Diesel particulate filters for light-duty vehicles: operation, maintenance, repair, and inspection.* TNO. Retrieved from http://publications.tno.nl/publication/34622025/OcBd1u/TNO-2016-R10958.pdf

unece.org. (2018, 01 09-12). *Informal document GRPE-76-08.* Retrieved from unece.org: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grpe/GRPE-76-08e.pdf

9 Annex A – Confidentiality Agreement

Confidentiality Agreement

Research data shared between the researchers in the DIAS project may contain personal identifiable information, the usage of which is protected by law. To comply with this law, usage and sharing of data is restricted and it is essential that you follow the rules and guidelines described in the ethical guidelines defined for DIAS for collecting, processing, sharing and storage of data.

In addition to this you are obliged to comply with the following terms:

- I will not share the participant data collected by the project team with any third parties, including the case study organisations, employers of the participants, or other members of the consortium of the DIAS project without explicit, written consent from the person(s) who provided the data.
- Where relevant, I will instruct the people for whom I have responsibility who have access to the data of the relevant ethical protocols and ensure that they follow the guidelines defined for the project, as listed below.
- I will delete the data at least _____ months after the project outcomes have been published (recommended time is 3 months).

Declaration: I hereby declare my consent with the rules outlined above:

Date: .....

Name & Organisation: .....

Signature: .....

List of persons in my organisation who have access to the data:
