DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D5.2
Deliverable Title	Advanced detection system against known tampering (Level 2)
Issue Date	31/12/2021
Dissemination level	Confidential
Main Author(s)	Andreas Hastall, Robert Bosch GmbH Jan Rheingans, Robert Bosch GmbH Hauke Wendt, Robert Bosch GmbH Robin Vermeulen, TNO
Version	V1.0

DIAS Consortium

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

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.

Executive summary

Exhaust aftertreatment systems (EATS) like Selective Catalytic Reduction (SCR), Diesel Particulate Filter (DPF) or Three-Way Catalyst (TWC) have helped to decrease the environmental impact of passenger cars, commercial vehicles and non-road mobile machinery over the last decades.

Irresponsible vehicle operators are performing changes in-vehicle hardware and software. Their aim is to deactivate these systems in order to reduce the total cost of ownership e.g. by reducing money spent on consumables or preventing replacement of faulty components. These changes are referred to as tampering and tackled by the EU H2020 project "DIAS – Smart Adaptive Remote Diagnostic Antitampering Systems". With a multilevel approach of complementary security and diagnostic measures, tampering should be prevented or detected.

The development of in-vehicle security measures and diagnostic features was documented in recent DIAS deliverables D4.2 and D5.1. It was concluded that the tampering devices identified in the DIAS work packages WP2 and WP3 can either be prevented from working or detected.

The original description of task 5.2 proposed to close any gaps in the prevention or detection of known tampering with a cloud-supported approach. Since there do not seem to be any remaining gaps, this report describes the Overall Diagnostic System (ODS) of tampering detection and tampering reporting. This system is designed to incorporate detection methods for future tampering, which is currently not known. These detection methods will be documented in the dedicated DIAS deliverable D5.3.

Potential future cloud-based services like tracking fleet emissions require data integrity. Security measures are crucial for this, but also diagnostic information is needed to judge whether a vehicle has been tampered with or not. A proposal of parameters that are relevant for one prototypic use-case includes:

- Secure SW and calibration identifier
- Tampering indicator value (as described in D5.1)
- Data verification status (from secure in-vehicle communication)
- Metadata (e.g. DTCs and milage)

Other parameters might be required for other cloud-based services.

A scheme for efficient emission reporting is presented in this work. It embraces aspects of CARB´s REAL approach and schemes from emission testing on test benches.

A prototypical demonstrator was finally set up in an open-source environment. Eclipse KUKSA can be deployed on a RaspberryPi and makes development access easy for all partners involved in DIAS. It uses the W3C vehicle signal specification as proposed by the Connected Vehicle Systems Alliance (COVESA).