DIAS

Smart Adaptive Remote Diagnostic Antitampering Systems

EUROPEAN COMMISSION

HORIZON 2020

LC-MG-1-4-2018

Grant agreement ID: 814951

Deliverable No.	D5.1
Deliverable Title	Enhanced diagnostic system based on conventional improved techniques (Level 1)
Issue Date	31/05/2021
Dissemination level	Confidential
Main Author(s)	Andreas Hastall, Robert Bosch GmbH Dinçer Özcan, Ford Otosan
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.

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 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.

Recent deliverables of DIAS have documented the market assessment of available tampering solutions (D3.1 and D3.2), a security assessment for a generic vehicle architecture (D4.1), proposals for future functional requirements to end-users (D2.2) and in-vehicular security techniques (D4.2).

The present report D5.1 is documenting the complementary development of an improved in-vehicular diagnostic system, addressing known tampering techniques. Given the control unit-based nature of these in-vehicular measures, only attacks using emulators or physical modifiers are considered. The issue of unauthorized flashing of altered ECU software is currently more relevant according to tamperers, but must be prevented or detected by advanced security measures.

While On Board Diagnostic (OBD) functions are intended to find faulty components, tampering very often tries to simulate a well-working system. This is why besides improvements of OBD functions dedicated tampering detection functions had to be developed in a prototypical way within the course of the underlying task 5.1.

According to the previous deliverables, advanced rationality checks were investigated to identify tampering with the following environmental protection systems (sorted by importance):

- SCR
- DPF
- TWC

System emulators have been found to use a variety of attacks to trick complex control systems. To identify the malicious deactivation of an aftertreatment system it is not necessary to detect every single attack path, but the ensemble. In some cases, finding the weakest spot of an emulator is sufficient, but relying on single features will raise the risk for false positive diagnoses. In order to mitigate these uncertainties in tampering detection a calibratable decision logic is proposed, which estimates a tampering probability from the individual detection modules mentioned above.

Although it is estimated, that with the prototypical functions presented, all modifiers and system emulators found by DIAS work package 2 and 3 would have been detected, it can be assumed, that with higher hurdles, tampering will become more sophisticated in the future as well.

A diagnostic system that can adapt to these new threats will be developed in the upcoming task 5.2 and documented in the corresponding deliverable 5.2.