DIAS

SMART ADAPTIVE
REMOTE DIAGNOSTIC
ANTITAMPERING
SYSTEMS

Two-pager

Tampered vehicles are defined as vehicles having their environmental protection system (EPS) manipulated by hardware or software means with the purpose to (partly) deactivate or bypass it. Numerous studies show a growing number of tampered vehicles worldwide and, considering that tampered vehicles contribute excessively to poor air quality and adverse effects on human health, tampering constitutes a serious environmental threat. The emissions impact of tampering depends on the original vehicle design and the extent of the vehicle modifications. For example, air pollution from a diesel vehicle increases drastically (tens or hundreds of times, depending on the pollutant) when its emissions controls are removed. It is important to note that the main motivation for vehicle's owner or operator for tampering is the economic advantages.

DIAS aims to harden vehicles' EPS against tampering. To do this, DIAS took a two-step approach: a first one focusing on implementing measures that take early action against these activities and a second one focusing on developing technologies that will address future tampering attempts. These systems and technologies are intended to operate throughout Europe and even on a global scale and will take advantage of future connectivity. The overall objective is to support the transition to more effective tampering protection and detection systems that will ensure a strong reduction of tampering activities and, to the extent possible, tamper-proof On-board Diagnostics (OBD) and On-board Monitoring of tailpipe pollutant emissions (OBM).

DIAS confirmed that tampering (with or without the help of an expert technician) is possible, even for vehicles complying with the current Euro standards and that tampering results in extreme increases in emissions. The project proposes guidelines and recommendations for future anti-tampering legislation as an anti-tampering framework including several involved entities and defining the role and guidelines addressed to each entity.

DIAS explored the subject in various dimensions including market and security analysis, identification of the detection methods and counter-measures, testing and demonstration of the success of measures and integration into future legislation. The whole effort was divided into certain work packages (WP) which covered a variety of activities designed to define and demonstrate the best available technology and to provide guidelines for legislation. To meet the project objectives every WP has been divided into particular tasks and related deliverables to be carried out by the beneficiaries.

Market and threat analysis has been performed to identify current tampering practices, determine existing EPSs' vulnerabilities, and quantify the risks and impacts of tampering on system functionality. Performing such a market assessment led to insights into the most effective cheating devices and their impact on emissions, OBD and vehicle systems and signals. The cheating devices were categorized per working principle and application and prioritized for subsequent testing to disclose the working principles of the tampering and the vulnerabilities of existing EPSs. It is strongly indicated that the main motive for tampering is to avoid costs for repair of malfunctions of the emissions control systems (SCR, DPF, EGR for diesel engines but possibly also TWC for older gasoline engines).

The vulnerabilities derived from tampering market and threat analysis were addressed by developing technical solutions for tampering detection (by monitoring and plausibility checks of EPS-related signals), prevention (by securing flashing process, SW execution, key management, and data exchange, and applying intrusion detection system and firewall) and reporting (by providing options for reporting schemes, infrastructure and tampering-related compliance certification).

DIAS solutions were evaluated against technology neutrality and applicability industry-wide, complexity, lead time, and cost (for development and operation). Most solutions were found neutral building upon common automotive technology, published scientific knowledge, worldwide accepted standards and protocols, and

EU or non-EU regulatory frameworks. Several of these were also evaluated as simple, low-cost and available in the short-term. The success of DIAS solutions was demonstrated through traditional penetration testing (internal evaluation), but also through two hacking events by independent experts (external evaluation) and no critical remaining vulnerabilities were observed.

Ultimately, based on the findings during the whole period of the project, an anti-tampering framework was proposed that incorporates guidelines for future anti-tampering legislation and engages several entities involved in anti-tampering. European Union Member States enforce the tampering-related EU regulatory framework. Vehicle manufacturers provide vehicle anti-tampering solutions for tampering prevention, detection and reporting for and after the Type Approval. Type approval and other authorities (i.e. Periodic Technical Inspection, Roadside Inspection) ensure and control the implementation of these solutions. Workshops ensure legitimate use of diagnostic tools and report tampering, and at last, vehicle owners ensure proper and timely maintenance and proper "reverting" actions if tampering is concluded.

Throughout the project, the consortium was working on generating awareness about the project, its objectives, and expected outcomes through different channels, and on identifying key stakeholders to consolidate a strong message for the potential interest and relation of our target audiences. In addition, the digital network has been an essential channel to amplify the reach to stakeholders, always placing first a creative and relevant content strategy. The storytelling around DIAS has been based on the demonstration of the tampering countermeasure success in events, webinars and through scientific publications. In addition, the consortium has generated several dissemination materials with a special focus on promoting the results in a friendly way through the development of videos, targeting developers and end-users to promote and demonstrate the capabilities of DIAS.

DIAS envisioned several layers of defense against currently known and unknown tampering practices. It also developed systems to incorporate detection methods for future tampering, which is currently not known. One of the challenges to beat future tampering lied in detecting these advanced yet unknown simulation techniques designed to hide the modification or intervention in the aftertreatment system components and cheat even the already existing detection systems.

Addressing the ultimate goal of the DIAS project to provide a set of guidelines and recommendations for future anti-tampering legislation, an anti-tampering framework has been developed. The framework and the developed detection methodology can be used for different types of vehicles, following the steps of the proposed workflow. However, in order to be applied to future vehicles, the structure of the detection systems may require changes and adaptations. New detectors can be added, or the proposed ones can be changed.

Over the 2022-2050 period, the maximum theoretical benefits that can be achieved in an ideal case where 100% of the tampering is eliminated, and based on the most realistic estimations for tampering shares and rates are:

- 3.7 megatons savings on NOx emissions
- 41 kilotons savings on PM emissions
- 26,000 avoided premature deaths
- 460,000 avoided years of life lost

The potential benefit is still significant, even if reduced by 10-25%, in case of a faster replacement of internal combustion engine vehicles from ZEVs. Most optimistic estimations for tampering shares and rates result in circa half benefit, while, if the highest available tampering shares and rates are used, the benefit doubles or even triples (e.g. 81,000 premature deaths can be avoided). It is also worth notable that while a decrease with time is expected in overall pollutant emissions and the associated health burden, the share associated with tampering is expected to increase. Therefore, tampering is expected to still contribute to a significant health burden in 2050 and anti-tampering legislation seems to have a key role to mitigate this.

A robust estimate of the monetary impact of tampering and, in particular, of the costs of the anti-tampering measures' development and implementation, was not feasible via DIAS project research, but follow-up projects could contribute to this effort.